M208

Pure mathematics

Book A

Introduction

This publication forms part of an Open University module. Details of this and other Open University modules can be obtained from Student Recruitment, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)300 303 5303; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2018.

Edited, designed and typeset by The Open University, using LaTeX.

Printed in the United Kingdom by Hobbs the Printers Limited, Brunel Road, Totton, Hampshire, SO40 3WX.

ISBN 978 1 4730 2266 9

2.1

Contents

Unit A1

Sets, functions and vectors

Introduction to Book A

M208 covers a wide range of pure mathematics, and each book apart from this one concentrates on one topic. This book is different, because it covers the main concepts that underlie the topics in the other books.

In Unit A1 you will review some of the important foundations of pure mathematics and the mathematical language used to describe them. You will start with the plane, and revise ideas relating to points, lines and circles. You will then study in detail the mathematical ideas of a *set* (mostly of numbers or of points in the plane), and a *function*, including functions of real numbers and functions of points in the plane. Finally, you will consider *vectors* in the plane and in three-dimensional space.

In Unit A2 you will look at number systems and their properties. You will first consider *real numbers*, and sets of real numbers, such as the integers and the rational numbers, then study *complex numbers*, investigate their properties, and look at some functions of complex numbers. Finally, you will study *modular arithmetic*, which provides examples of *finite* number systems.

In Unit A3 you will concentrate on mathematical language and communication. You will study the important subject of mathematical proof, including the use of different methods of proof, and how to disprove a statement by finding a counterexample. You will also consider errors in mathematical arguments including errors in deduction. Finally, you will study *equivalence relations* and the idea of a *partition* of a set.

In Unit A4 you will concentrate on *real functions*, and on how to draw their graphs. You will review the graphs of various common functions, and consider a wide range of functions and their properties, including *trigonometric* and *hyperbolic functions*. Finally, you will consider curves that are not the graphs of real functions including *conics* (circles, parabolas, hyperbolas and ellipses) and see that they can be described in terms of a single parameter.

Introduction

In this unit you will look at some of the most fundamental mathematical concepts underlying pure mathematics. Many of these concepts should not be new to you, but working through this unit should ensure that you understand them to the level needed for M208.

Sections 1 to 3 contain basic material that will be crucial throughout the module. It is vital that you become familiar and confident with the ideas and notation introduced in these sections. Section 4 revises concepts that will be used later in the module, in particular in Book C *Linear algebra*.

1 Points, lines and distance

In this section you will revise points, lines and distance in two- and three-dimensional space.

1.1 The plane

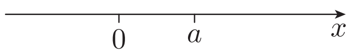


Figure 1 The real line

The set of all real numbers is denoted by $\mathbb{R}$, and this set can be pictured as an infinitely long number line, often called the **real line**, as shown in Figure 1. Each real number a corresponds to a point on the line.

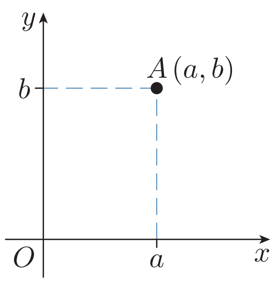


Figure 2 Cartesian coordinates

In this subsection we consider **the plane**, or two-dimensional space. To allow us to specify the locations of points in the plane, we usually use a pair of perpendicular axes, known as **Cartesian** or **rectangular** axes. We usually label the axes x and y; we refer to their intersection point as the **origin** and sometimes label it O. Finally, we choose a unit of distance. The location of any **point** in the plane can be specified by using an ordered pair (a, b) of real numbers, known as **Cartesian coordinates** or just **coordinates**, that give the position of the point relative to the axes, as shown in Figure 2. (An **ordered pair** is a pair in which order matters; for example, the ordered pair $(2, 3)$ is different from the ordered pair $(3, 2)$.) We write $A(a, b)$ to specify the point A with coordinates (a, b).

It is important to understand that the coordinates of a point depend on where the axes have been placed in the plane; if we had chosen the axes to be in a different position, then usually the coordinates of the point would be different. However, once we have chosen the position of the axes, we often do not bother to distinguish explicitly between a point and its representation using these coordinates: we simply write (a, b) to denote the point A.

We use the notation $\mathbb{R}^2$ to denote the plane.

René Descartes

The adjective Cartesian comes from the surname of the French mathematician and philosopher René Descartes (1596–1650). He was the first person to show in print how algebra could be used to study geometry, in his 1637 publication *La géométrie*. Descartes' procedure differed from the system of Cartesian coordinates that we use today. His axes were not necessarily at right angles, and could be chosen in relation to the circumstances of the problem rather than being given in advance.

The plane, together with an **origin** O and a pair of x- and y-axes, is known as **two-dimensional Euclidean space**.

Euclidean space is named after the Greek mathematician Euclid. Little is known for certain about Euclid but he is believed to have worked in Alexandria in around 300 BCE.

Euclid's *Elements*, a mathematical treatise of thirteen books which had its origins on papyrus rolls, has become one of the most frequently printed texts of all time. Although *Elements* covers both plane and solid Euclidean geometry, Euclid had no notion of axes or coordinates.

Lines

The equation of any straight line in $\mathbb{R}^2$, except a line parallel to the y-axis, can be written in the form

$$y = mx + c,$$

where $m, c \in \mathbb{R}$.

In this equation:

- m is the **gradient** (or *slope*) of the line, given by
$$m = \frac{y_2 - y_1}{x_2 - x_1}, \tag{1}$$
where (x_1, y_1) and (x_2, y_2) are any two points on the line such that $x_1 \neq x_2$
- c is the **y-intercept** of the line; that is, $(0, c)$ is the point at which the line crosses the y-axis, as illustrated in Figure 3(a).

The line with gradient m that crosses the y-axis at the origin has equation $y = mx$, since $c = 0$ in this case; see Figure 3(b). The horizontal line (parallel to the x-axis) with y-intercept c has equation $y = c$, since the gradient $m = 0$ in this case; see Figure 3(c).

The equation of a line parallel to the y-axis cannot be written in the form (1). The vertical line (parallel to the y-axis) with x-intercept a has equation $x = a$; see Figure 3(d). The equation of such a line cannot be written in the form $y = mx + c$ because the gradient is undefined.

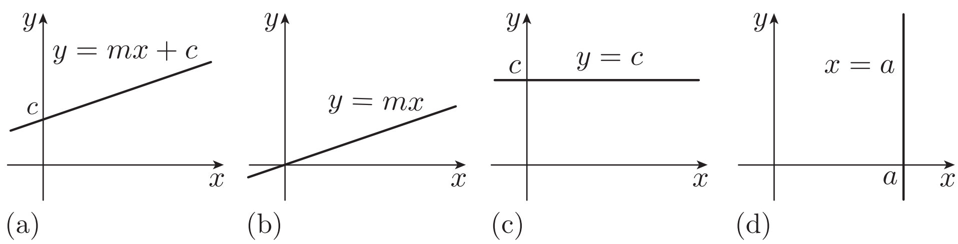


Figure 3 Lines in the plane

In all of the cases above, the equation of the line in the plane can be rearranged to take the form

$$ax + by = c, \tag{2}$$

for some real numbers a, b and c, where a and b are not both zero. (Note that the numbers a and c here are not the same as those called a and c in Figure 3.)

In fact, any line in $\mathbb{R}^2$ has an equation of the form (2) and, conversely, any equation of the form (2) represents a line in $\mathbb{R}^2$.

Equation of a line

The general equation of a line in $\mathbb{R}^2$ is

$$ax + by = c,$$

where a, b and c are real numbers, and a and b are not both zero.

From formula (1) for the gradient of a line, we can see that the equation of the line with gradient m that passes through the point (x_1, y_1) is

$$y - y_1 = m(x - x_1).$$

Exercise A1

Determine the equation of the line with gradient -3 that passes through the point $(2, -1)$.

Exercise A2

Determine the equation of the line through each of the following pairs of points.

(a) $(1, 1)$ and $(3, 5)$ (b) $(0, 0)$ and $(0, 8)$ (c) $(0, 0)$ and $(4, 2)$

(d) $(4, -1)$ and $(2, -1)$

Parallel and perpendicular lines

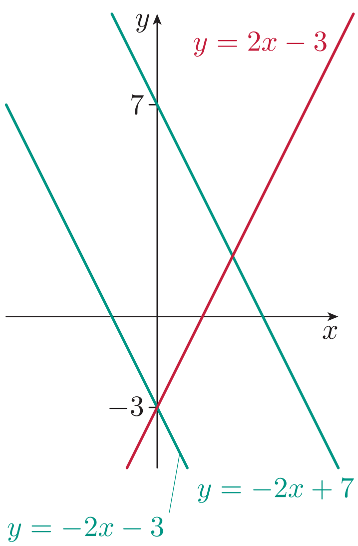


Figure 4 Parallel and perpendicular lines

Two distinct lines are **parallel** if they never meet, and **perpendicular** if they meet at right angles.

Saying that two non-vertical lines are parallel is equivalent to saying that they have the same gradient but different y-intercepts. For example, as shown in Figure 4, the lines $y = -2x + 7$ and $y = -2x - 3$ are parallel since they both have gradient -2 but their y-intercepts are 7 and -3, respectively, whereas the lines $y = -2x + 7$ and $y = 2x - 3$ are not parallel since their gradients -2 and 2 are not equal.

We can also use the gradients of a pair of non-vertical lines to check whether they are perpendicular, as follows.

Gradients of perpendicular lines

Let l_1 and l_2 be lines with gradients m_1 and m_2, respectively.

- If l_1 and l_2 are perpendicular, then $m_1 m_2 = -1$.
- If $m_1 m_2 = -1$, then l_1 and l_2 are perpendicular.

To see that the first statement in the box is true, suppose that the lines l_1 and l_2 are perpendicular and that neither line is vertical. Let the gradients of l_1 and l_2 be m_1 and m_2, respectively. Then one of the lines (l_1, say) must slope up from left to right and the other (l_2, say) must slope down from left to right, as shown in Figure 5.

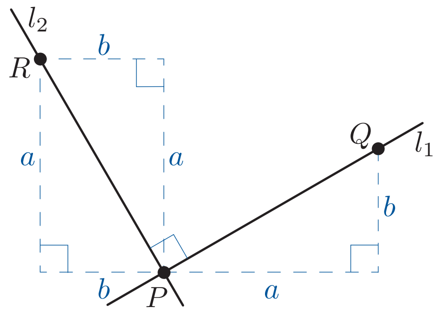


Figure 5 Perpendicular lines

Let the lines intersect at P, and let Q be a point on l_1 to the right of P. Suppose that Q is a units to the right of P and b units up from P, as illustrated in Figure 5. Let R be the point on l_2 obtained by rotating PQ anticlockwise through a right angle; then R is b units to the left of P and a units up from P, as shown.

It follows that the gradient of l_1 is $m_1 = b/a$, and the gradient of l_2 is $m_2 = -a/b$. Hence

$$m_1 m_2 = \frac{b}{a} \times \left(-\frac{a}{b}\right) = -1.$$

The proof of the second statement in the box above is not given here.

Worked Exercise A1

Determine which of the following lines are parallel, and which are perpendicular to each other.

$$l_1\colon\ y = -2x + 4 \qquad l_2\colon\ 2x - 3y - 2 = 0 \qquad l_3\colon\ y - 2x = 9$$
$$l_4\colon\ 2y + 3x + 5 = 0 \qquad l_5\colon\ x + \tfrac{1}{2}y + 2 = 0 \qquad l_6\colon\ 2y = 3x + 7$$

Solution

We can rearrange the equations of the lines to find their gradients as follows.

$$l_1\colon\ y = -2x + 4 \qquad l_2\colon\ y = \tfrac{2}{3}x - \tfrac{2}{3} \qquad l_3\colon\ y = 2x + 9$$
$$l_4\colon\ y = -\tfrac{3}{2}x - \tfrac{5}{2} \qquad l_5\colon\ y = -2x - 4 \qquad l_6\colon\ y = \tfrac{3}{2}x + \tfrac{7}{2}$$

Thus the gradients of the lines are -2, $\frac{2}{3}$, 2, $-\frac{3}{2}$, -2 and $\frac{3}{2}$, respectively.

The gradients of l_1 and l_5 are equal, and since their y-intercepts are different, the lines l_1 and l_5 are parallel. Multiplying the gradients of l_2 and l_4 gives $\frac{2}{3} \times \left(-\frac{3}{2}\right) = -1$, so the lines l_2 and l_4 are perpendicular.

Exercise A3

Determine which of the following lines are parallel, and which are perpendicular to each other.

l_1: $y = -2x + 4$	l_2: $6x - 3y + 4 = 0$	l_3: $2y + x = 10$
l_4: $6y - 3x + 5 = 0$	l_5: $x - 2y + 2 = 0$	l_6: $2y + 4x + 7 = 0$

Distance between two points in the plane

Next, we find the formula for the distance between any two points in the plane.

We use the idea of the **modulus** of a real number k, written $|k|$ and defined by

$$|k| = \begin{cases} k, & \text{if } k \geq 0, \\ -k, & \text{if } k < 0. \end{cases}$$

(The modulus of k, usually read as 'mod k' is sometimes called the **absolute value** or **magnitude** of k.)

Suppose that $P(x_1, y_1)$ and $Q(x_2, y_2)$ are two points in the plane, as shown in Figure 6. We can construct a right-angled triangle PNQ as shown: the line PN is parallel to the x-axis, the line QN is parallel to the y-axis, the angle PNQ is a right angle, and PQ is the hypotenuse of the triangle. In Figure 6, P and Q are drawn in the first quadrant and with PQ sloping up from left to right, but the formula holds wherever the points are in the plane.

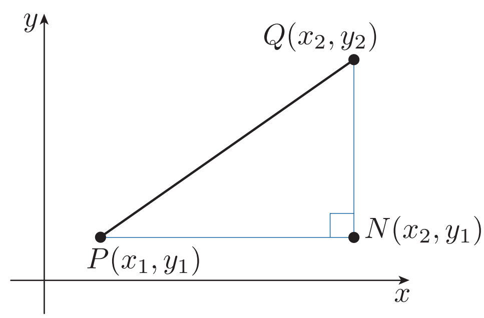


Figure 6 Distance between P and Q in the plane

The length of PN is $|x_2 - x_1|$ and the length of QN is $|y_2 - y_1|$. It follows from Pythagoras' Theorem that

$$PQ^2 = PN^2 + QN^2,$$

and since $|k|^2 = k^2$ for any real number k, we have

$$PQ = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

Distance formula for $\mathbb{R}^2$

The distance between the two points (x_1, y_1) and (x_2, y_2) in the plane is

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

For example, it follows from the formula above that the distance between the points $(1, 2)$ and $(3, -4)$ is

$$\begin{aligned}\sqrt{(3-1)^2 + (-4-2)^2} &= \sqrt{2^2 + (-6)^2} \\ &= \sqrt{40} = \sqrt{4 \times 10} \\ &= \sqrt{4}\sqrt{10} = 2\sqrt{10}.\end{aligned}$$

Exercise A4

Find the distances between the following pairs of points in the plane.

(a) $(0, 0)$ and $(5, 0)$ (b) $(0, 0)$ and $(3, 4)$ (c) $(1, 2)$ and $(5, 1)$

(d) $(3, -8)$ and $(-1, 4)$

Circles

A **circle** in $\mathbb{R}^2$, as illustrated in Figure 7, is the set of points $P(x, y)$ that lie at a fixed distance r, called the **radius**, from a fixed point $C(a, b)$, called the **centre** of the circle.

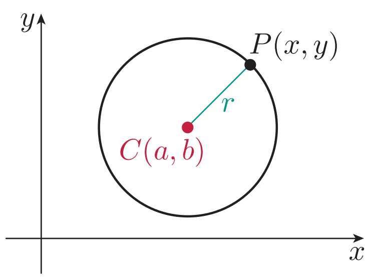


Figure 7 A circle with radius r and centre (a, b)

By the distance formula, every point (x, y) on the circle with centre (a, b) and radius r satisfies the equation

$$\sqrt{(x-a)^2 + (y-b)^2} = r.$$

Squaring this equation to remove the square root gives the following.

Equation of a circle

The equation of the circle in $\mathbb{R}^2$ with centre (a, b) and radius r is

$$(x-a)^2 + (y-b)^2 = r^2.$$

In this unit we will just work with equations of circles in this form, without multiplying out the brackets. In Unit A4 *Real functions, graphs and conics*, you will see how multiplying out the brackets leads to other forms for the equations of circles.

Worked Exercise A2

Find the equation of the circle with centre $(-1, 2)$ and radius $\sqrt{3}$.

Solution

The circle has equation

$$(x - (-1))^2 + (y - 2)^2 = (\sqrt{3})^2,$$

that is,

$$(x + 1)^2 + (y - 2)^2 = 3.$$

Exercise A5

Determine the equation of each of the following circles, given the centre and radius.

(a) Centre the origin, radius 4.

(b) Centre $(-1, 0)$, radius $\sqrt{2}$.

(c) Centre $(3, -4)$, radius 2.

1.2 Three-dimensional space

We now look briefly at three-dimensional space.

We define a coordinate system in three-dimensional space using three *mutually perpendicular* axes. The word *mutually* here means that the condition holds for any pair, so **mutually perpendicular** means that any two of the axes are perpendicular.

First, we choose a point O as the origin, and then we choose an x-axis and a y-axis at right angles to each other. Next, we draw a third line through the origin, perpendicular both to the x-axis and to the y-axis; this line is called the z-axis. We choose the positive direction of the z-axis to be such that the x-, y- and z-axes form a so-called **right-handed system of axes**. This means that if you hold the thumb and first and second fingers of your right hand at right angles to each other, and label them x, y and z, in that order, then you can turn your hand in such a way that your fingers point in the positive directions of the corresponding axes, as shown in Figure 8.

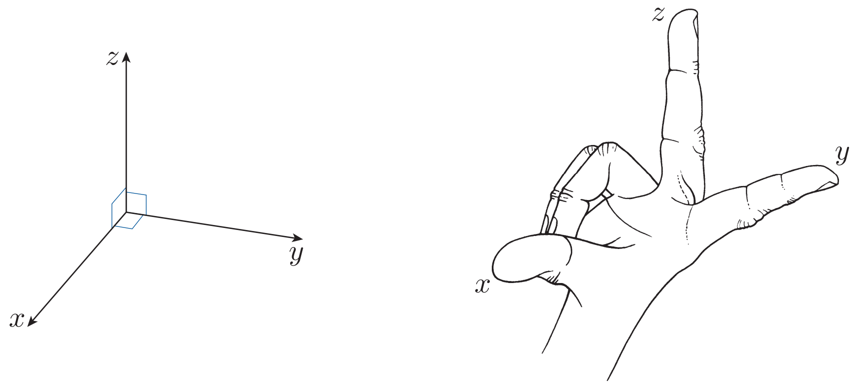


Figure 8 A right-handed system of coordinate axes for $\mathbb{R}^3$

Finally, we choose a unit of distance.

We represent each point in three-dimensional space by an **ordered triple** (a, b, c) of real numbers. The point with coordinates (a, b, c) is reached from the origin by moving a distance a in the direction of the x-axis, a distance b in the direction of the y-axis, and a distance c in the direction of the z-axis, as illustrated in Figure 9(a).

For instance, the point with coordinates $(-3, -2, 4)$ is shown in Figure 9(b).

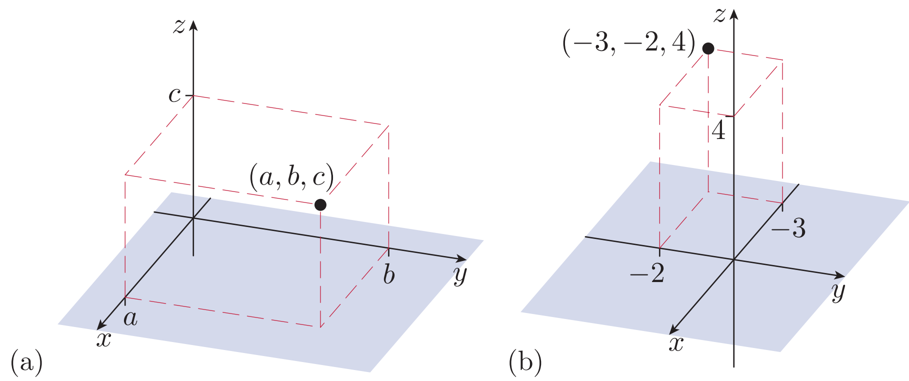


Figure 9 Three-dimensional Cartesian coordinates

In Figure 9, the plane containing the x-axis and the y-axis is shaded. Usually we think of this plane as being horizontal, and the z-axis as being vertical.

We use the notation $\mathbb{R}^3$ to denote three-dimensional space.

Exercise A6

Sketch the x-, y- and z-axes and the points with coordinates $(0, 1, 2)$ and $(-1, 2, -1)$.

As with $\mathbb{R}^2$, once we have chosen the position of the axes, we often do not bother to distinguish explicitly between a point and its representation using these coordinates; we simply write (a, b, c) to denote the point in $\mathbb{R}^3$ represented by this triple.

Three-dimensional space, together with an origin and a set of x-, y- and z-axes, is known as **three-dimensional Euclidean space**.

Distance between points in $\mathbb{R}^3$

You saw in Subsection 1.1 that the distance between two points (x_1, y_1) and (x_2, y_2) in the plane is given by

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

We can establish a similar formula for the distance between two points in $\mathbb{R}^3$, as follows.

Let $P(x_1, y_1, z_1)$ and $Q(x_2, y_2, z_2)$ be two points in $\mathbb{R}^3$. Let M be the point (x_2, y_2, z_1); then M lies in the same horizontal plane as P, and MQ is parallel to the z-axis. Next, let N be the point (x_1, y_2, z_1); then N also lies in the same horizontal plane as P, and MN and NP are parallel to the x- and y-axes, respectively.

The triangles PQM and PMN are both right-angled triangles, with right angles at M and N, respectively, as shown in Figure 10.

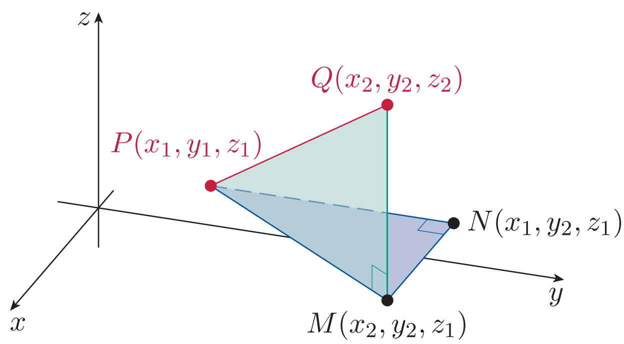


Figure 10 Distance between P and Q in $\mathbb{R}^3$

The length of PN is $|y_2 - y_1|$ and the length of NM is $|x_2 - x_1|$. It follows from Pythagoras' Theorem that

$$PM^2 = NM^2 + PN^2,$$

so

$$PM^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2.$$

Using Pythagoras' Theorem again gives

$$PQ^2 = PM^2 + MQ^2,$$

and since the length of MQ is $|z_2 - z_1|$ we obtain

$$PQ^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2,$$

that is,

$$PQ = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}.$$

Distance formula for $\mathbb{R}^3$

The distance between the two points (x_1, y_1, z_1) and (x_2, y_2, z_2) in $\mathbb{R}^3$ is

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}.$$

For example, it follows from this formula that the distance between the points $(1, 2, 3)$ and $(4, -2, 15)$ is

$$\sqrt{(4-1)^2 + (-2-2)^2 + (15-3)^2} = \sqrt{169} = 13.$$

Exercise A7

Find the distances between the following pairs of points in $\mathbb{R}^3$.

(a) $(1, 1, 1)$ and $(4, 1, -3)$ (b) $(1, 2, 3)$ and $(3, 0, 3)$

We will return to the topic of three-dimensional space in Section 4, where we will consider vectors in $\mathbb{R}^3$ as well as in $\mathbb{R}^2$, and find the general equation of a plane in $\mathbb{R}^3$.

2 Sets

In this section you will revise the notion of sets, learn new notation for describing sets, and practise working with sets and set notation. These skills will be crucial in the rest of the module.

2.1 What is a set?

In mathematics we frequently work with collections of objects of various kinds. We may, for example, consider the following:

- solutions of a quadratic equation
- points on a circle
- vertices of a triangle
- points on a plane in $\mathbb{R}^3$
- even numbers less than 100
- students taking a particular examination.

The concept of a *set* allows us to work with such collections systematically.

You can think of a **set** as a collection of objects, such as numbers, points, functions, or even a collection of other sets. Each object in a set is an **element** or **member** of the set, and the elements *belong to* the set, or are *in* the set.

There is no restriction on the types of object that may appear in a set, provided that the set is specified in a way that enables us to decide, in principle, whether a given object is in the set.

There are many ways of making such a specification. For example, we can define S to be the set of numbers in the list

$$4, \ 9, \ 3, \ 2.$$

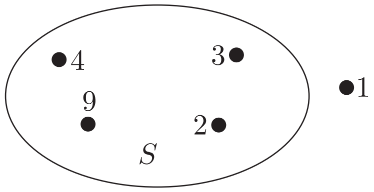


Figure 11 A Venn diagram of the set S

This enables us to decide that the number 2 (say) is in S, but that the number 1 (say) is not in S. We can illustrate this set by a diagram, as in Figure 11, where the symbol S is *not* a member of the set but a label for it. (Similar labels will appear in other diagrams.) Such a diagram is called a **Venn diagram**, after the nineteenth-century Cambridge mathematician John Venn.

We can also define a set by describing its elements; for example,

let E be the set of all even integers.

This description enables us to determine whether a given object is in E by deciding whether it is an even integer; for example, 6 is in E, but 5 is not.

Some sets are used so often that special symbols are reserved for them. Recall that a **real number** is a number with a decimal expansion (possibly infinite), for example, 1.1 or $\pi = 3.14\ldots$, and a **rational number** is a real number that can be expressed as a fraction, for example, 14/5 or $-3/4$. You will revise these sets more thoroughly in Unit A2 *Number systems*. We use the following notation, some of which you met in Section 1.

$\mathbb{R}$ denotes the set of real numbers.

$\mathbb{R}^*$ denotes the set of non-zero real numbers.

$\mathbb{Q}$ denotes the set of rational numbers.

$\mathbb{Z}$ denotes the set of integers $\ldots, -2, -1, 0, 1, 2, \ldots$.

$\mathbb{N}$ denotes the set of natural numbers $1, 2, 3, \ldots$.

A **finite set** is a set that has a finite number of elements; that is, the number of elements is some natural number, or 0. Any set that is not a finite set is an **infinite set**.

We use the symbol $\in$ to indicate membership of a set; for example, we indicate that 7 is a member of $\mathbb{N}$ by writing

$7 \in \mathbb{N}$. (This is usually read as '7 belongs to $\mathbb{N}$' or '7 is in $\mathbb{N}$'.)

We indicate that -9 is *not* a member of $\mathbb{N}$ by writing

$-9 \notin \mathbb{N}$. ('-9 does not belong to $\mathbb{N}$' or '-9 is not in $\mathbb{N}$'.)

We also use the symbol $\in$ when we wish to introduce a symbol that stands for an *arbitrary* (that is, general, unspecified) element of a set. For example, to indicate that x is a **real variable**, that is, an arbitrary member of the set $\mathbb{R}$, we write

let $x \in \mathbb{R}$.

We often write $x_1, x_2 \in S$ as shorthand to combine $x_1 \in S$ and $x_2 \in S$.

Exercise A8

Which of the following statements are true?

(a) $-3 \in \mathbb{Z}$ (b) $5 \notin \mathbb{N}$ (c) $1.3 \notin \mathbb{Q}$ (d) $1, 3 \in \mathbb{Q}$

(e) $-\pi \in \mathbb{R}$ (f) $\frac{1}{2} \in \mathbb{N}$ (g) $0, 1 \in \mathbb{R}^*$ (h) $\sqrt{2} \notin \mathbb{R}$

2.2 Set notation

We now look at some formal ways of specifying a set.

We can specify a set with a small number of elements by listing these elements between a pair of braces (curly brackets). For example, we can specify the set A consisting of the first five natural numbers, illustrated in Figure 12, by

$$A = \{1, 2, 3, 4, 5\}.$$

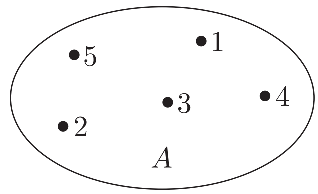


Figure 12 The set A

The membership of a set is not affected by the order in which its elements are listed, so we can specify this set A equally well by

$$A = \{5, 2, 1, 4, 3\}.$$

Similarly, we can specify the set B of vertices of the square shown in Figure 13 by

$$B = \{(0, 0), (1, 0), (1, 1), (0, 1)\}.$$

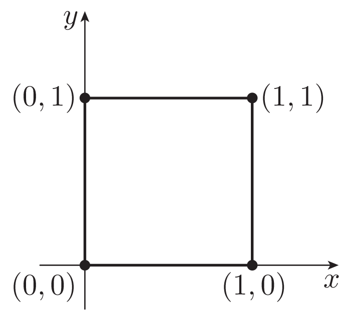


Figure 13 The set B

We can even specify a set C, illustrated in Figure 14, whose elements are the three sets $\{1, 3, 5\}$, $\{9, 4\}$ and $\{2\}$ by

$$C = \{\{1, 3, 5\}, \{9, 4\}, \{2\}\}.$$

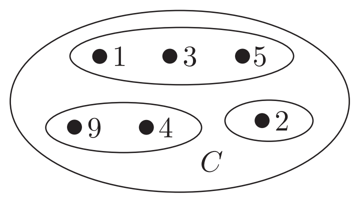


Figure 14 The set C

A set with only one element, such as the set $\{2\}$, is called a **singleton** or a **singleton set**. (Do not confuse the *set* $\{2\}$ which contains the number 2, with the *number* 2 itself.)

Exercise A9

Which of the following statements are true?

(a) $1 \in \{4, 3, 1, 7\}$

(b) $\{-9\} \in \{\{6, 1, 2\}, \{8, 7, 9, 5\}, \{-9\}, \{5, 4\}\}$

(c) $\{9\} \in \{5, 6, 7, 8, 9\}$

(d) $(0, 1) \in \{(1, 0), (1, 4), (2, 4)\}$

(e) $1, 0 \in \{(1, 0), (1, 4), (2, 4)\}$

(f) $\{1, 0\} \in \{\{0, 1\}, \{1, 4\}, \{2, 4\}\}$

It does not matter if we specify a set element more than once within set brackets. For example,

$$\{1, 2, 3, 3\} \quad \text{and} \quad \{1, 2, 3\}$$

describe the same set. However, we usually try to avoid specifying an element more than once.

For a set with a large number of elements, it is not practical to list all the elements, so we sometimes use three dots (called an **ellipsis**) to indicate that a particular pattern of membership continues. For example, we can specify the set consisting of the first 100 natural numbers by writing

$$\{1, 2, 3, \ldots, 100\}.$$

The use of an ellipsis can be extended to certain infinite sets. For example, we can specify the set of all natural numbers by writing

$$\{1, 2, 3, \ldots\}.$$

One disadvantage of this notation is that the pattern indicated by the ellipsis may be ambiguous. For example, it is not clear whether

$$\{3, 5, 7, \ldots\}$$

denotes the set of odd prime numbers or the set of odd natural numbers greater than 1. For this reason, this notation can be used only when the pattern of membership is obvious, or where an additional clarifying explanation is given.

An alternative way of specifying a set is to use variables to build up objects of the required type, and then write down the condition(s) that the variables must satisfy. For example, consider the set of all real numbers x such that $x > 3$. Using set notation, we write this as

$$\{x \in \mathbb{R} : x > 3\},$$

which is read as shown in Figure 15.

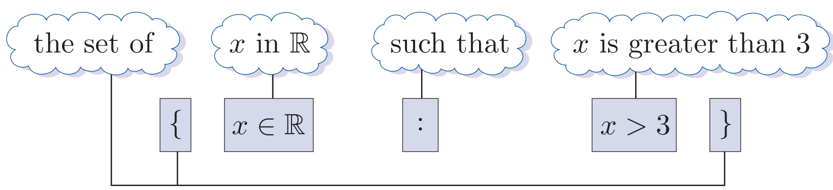


Figure 15 How to 'read' set notation

A set can often be described in several different ways using such set notation. In particular, we can use a letter other than x to denote an arbitrary (general) element of a set; for example, the set above can also be written as

$$\{r \in \mathbb{R} : r > 3\}.$$

If it is necessary to include more than one condition after the colon, then we write either a comma or the word 'and' between the conditions. So the

set of real numbers greater than 0, and less than or equal to 1, can be written as

$$\{x \in \mathbb{R} : x > 0,\ x \leq 1\} \quad \text{or} \quad \{x \in \mathbb{R} : x > 0 \text{ and } x \leq 1\},$$

although usually we combine the inequalities and write

$$\{x \in \mathbb{R} : 0 < x \leq 1\}.$$

Sometimes it is convenient to specify a set by writing an expression in one or more variables before the colon, and the conditions on the variables after the colon. For example, the set of even integers less than 100 may be specified by

$$\{2k : k \in \mathbb{Z} \text{ and } k < 50\}.$$

Just as when listing the elements of a set, it does not matter when using set notation if a set element is specified more than once. For example,

$$\{\sin x : x \in \mathbb{R}\}$$

specifies the same set as

$$\{\sin x : 0 \leq x < 2\pi\}.$$

Exercise A10

Which of the following statements are true?

(a) $\frac{9}{2} \in \{x \in \mathbb{R} : x > 3\}$ (b) $7 \in \{3k + 1 : k \in \mathbb{Z}\}$

(c) $-\frac{7}{2} \in \{x \in \mathbb{Z} : x < 5\}$ (d) $8 \in \{2^x : x \in \mathbb{R},\ 0 < x < 2\}$

(e) $9 \in \{n \in \mathbb{Z} : n = k^2 \text{ for some } k \in \mathbb{Z}\}$ (f) $6 \in \{m(m-1) : m \in \mathbb{N}\}$

(g) $4 \in \{r : r \text{ is an even integer},\ 0 < r < 4\}$

Notice that the next worked exercise contains lines of blue text, marked with the icons . You will see similar text in some of the worked exercises and proofs throughout this module. This text tells you what someone doing the mathematics might be thinking, but would not write down; or what a lecturer might say to explain the thinking behind the mathematics, but would not write on the board. It should help you understand how you might approach a similar exercise yourself.

Worked Exercise A3

Use set notation to specify each of the following.

(a) The set of all natural numbers greater than 50.

(b) The set of all odd integers.

Solution

(a) The elements of this set are the natural numbers n such that $n > 50$.

The set is $\{n \in \mathbb{N} : n > 50\}$.

(b) The odd integers are the numbers that can be written in the form $2k + 1$, for some integer k.

The set is $\{2k + 1 : k \in \mathbb{Z}\}$.

The choice of the variables is arbitrary in these sets, but k for an integer and n for a natural number are conventional.

Exercise A11

Use set notation to specify each of the following.

(a) The set of integers greater than -2 and less than 1000.

(b) The set of positive rational numbers with square greater than 2.

(c) The set of even natural numbers.

(d) The set of integer powers of 2.

Set notation is useful when we wish to refer to the set of solutions of one or more equations (called the **solution set**). For example, the real solutions of the equation $x^2 = 1$ form the set

$$\{x \in \mathbb{R} : x^2 = 1\} = \{-1, 1\}.$$

The solution set of an equation depends on the set of values from which the solutions are taken. For example, the solution set of the equation

$$(x-1)(2x-1) = 0$$

is

$$\{x \in \mathbb{R} : (x-1)(2x-1) = 0\} = \left\{1, \tfrac{1}{2}\right\}$$

if we are interested in real solutions. However, the solution set is

$$\{x \in \mathbb{Z} : (x-1)(2x-1) = 0\} = \{1\}$$

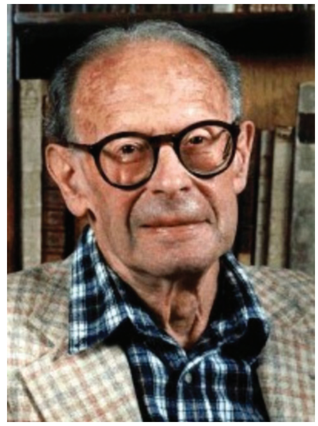
if we are interested only in integer solutions. In this unit we assume that solutions are taken from $\mathbb{R}$ unless otherwise stated.

Sometimes an equation has *no* real solutions, so its solution set has no elements.

The set with no elements arises frequently in mathematics, so it is given a special name and notation. It is called the **empty set** and is denoted by the symbol $\varnothing$. Thus, for example,

$$\{x \in \mathbb{R} : x^2 = -1\} = \varnothing.$$

The symbol for the empty set, $\varnothing$, was introduced in 1939 by the French mathematician André Weil (1906–1998), who took the symbol from the Norwegian alphabet.



André Weil

2.3 Intervals

You saw in Subsection 1.1 that the set of real numbers $\mathbb{R}$ can be pictured as a number line, called the real line. Many sets involve ranges of real numbers extending along the real line from one number a to another number b. Each of the endpoints a and b may be either included or excluded. Such sets are called **intervals** of the real line, and they occur so frequently that we use special notation for them. For example:

- the interval given by $-2 < x < 5$, in which both endpoints are *excluded*, is denoted by $(-2, 5)$ and is an example of an *open* interval
- the interval given by $-2 \leq x \leq 5$, in which both endpoints are *included*, is denoted by $[-2, 5]$ and is an example of a *closed* interval
- the intervals given by $-2 < x \leq 5$ and $-2 \leq x < 5$, in which one endpoint is included and the other is excluded, are denoted by $(-2, 5]$ and $[-2, 5)$, respectively, and are examples of *half-open* (or *half-closed*) intervals.

In some texts, a reversed square bracket is used instead of a round bracket to indicate an excluded endpoint; for example $]-2, 5[$ is used instead of $(-2, 5)$ for an open interval.

We use the symbol ∞ (infinity) when an interval extends indefinitely far to the right on the real line, and the symbol $-\infty$ when an interval extends indefinitely far to the left. For example:

- the set of all real numbers greater than -3 is denoted by $(-3, \infty)$
- the set of all real numbers less than or equal to 4 is denoted by $(-\infty, 4]$.

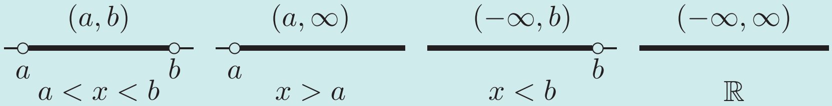
The symbol ∞ does not denote a real number: instead, it simply means that the interval continues indefinitely. We always use round brackets with ∞ and $-\infty$.

The notation for intervals is summarised in the box below.

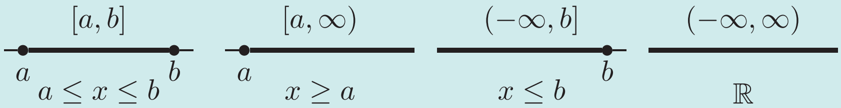
Interval notation

Intervals are denoted as follows.

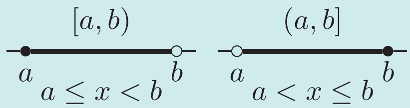
Open intervals



Closed intervals



Half-open (or half-closed) intervals



Remarks

1. In the box above, a hollow dot $\circ$ indicates that an endpoint is excluded, and a solid dot $\bullet$ indicates that an endpoint is included.
2. A singleton set $\{a\}$, containing a single number a, is a closed interval whose endpoints are equal.
3. An interval such as $[a, \infty)$ is regarded as closed, rather than half-open (or half-closed), because it contains *all* the real numbers greater than or equal to a. However, the interval $\mathbb{R} = (-\infty, \infty)$ is considered to be both open and closed.
4. We also use the notation (a, b) to denote a point in the plane, but in most cases it should be obvious whether a point or an interval is intended.

Exercise A12

Which of the following statements are true?

(a) $1 \in (1, 5)$ (b) $1 \in (-1, 1]$ (c) $\infty \in (0, \infty)$ (d) $0 \notin \mathbb{R}^*$

(e) If $x \in \mathbb{R}^*$, then $x \in (0, \infty)$.

Exercise A13

Use interval notation to specify the following intervals.

(a) 

(b) The set of real numbers x such that $-6.5 < x \le 21$.

(c) $\{x \in \mathbb{R} : x > -273\}$.

2.4 Plane sets

In Subsection 1.1 you met the plane $\mathbb{R}^2$, and saw that each point in the plane can be represented as an ordered pair (x, y) with respect to a chosen pair of axes. A set of points in $\mathbb{R}^2$ is called a **plane set** or a **plane figure**. The lines and circles that you met in Subsection 1.1 are simple examples of plane sets.

Lines as plane sets

Consider a straight line l_1 with gradient m and y-intercept c, as illustrated in Figure 16. This line is the set of all points (x, y) in the plane such that $y = mx + c$. Using set notation, we write this as

$$l_1 = \{(x, y) \in \mathbb{R}^2 : y = mx + c\}.$$

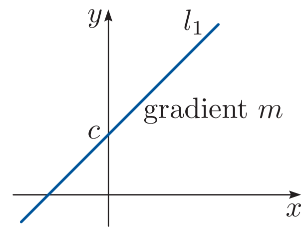


Figure 16 The line l_1

(We often refer to 'the line $y = mx + c$' as a shorthand way of specifying this set.)

For a line l_2 parallel to the y-axis with x-intercept a, as illustrated in Figure 17, we write

$$l_2 = \{(x, y) \in \mathbb{R}^2 : x = a\}.$$

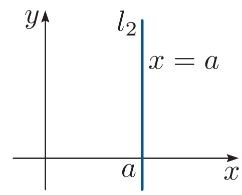


Figure 17 The vertical line l_2

An alternative way of specifying a line is to write an expression for one or both of the coordinates. For example, an alternative way of specifying the line l_1 with equation $y = mx + c$ is

$$l_1 = \{(x, mx + c) : x \in \mathbb{R}\}.$$

It does not matter what variable we use to specify the line. For example, we can also write

$$l_1 = \{(t, mt + c) : t \in \mathbb{R}\}.$$

Exercise A14

(a) Use set notation to specify the line l with gradient 2 that passes through the point $(0, 5)$.

(b) Sketch the line $l = \{(x, y) \in \mathbb{R}^2 : y = 1 - x\}$.

(c) Sketch the line $l = \{(x, x) : x \in \mathbb{R}\}$.

Circles as plane sets

Consider a circle C with centre (a, b) and radius r, as illustrated in Figure 18. This circle is the set of all points (x, y) in the plane such that $(x - a)^2 + (y - b)^2 = r^2$, so, in set notation, it can be written as

$$C = \{(x, y) \in \mathbb{R}^2 : (x - a)^2 + (y - b)^2 = r^2\}.$$

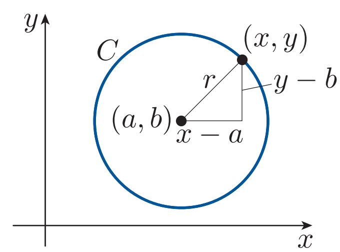


Figure 18 A circle C

The **unit circle** U is defined to be the circle centred at the origin with radius 1, so it is the set of points (x, y) in the plane whose distance from

the origin $(0,0)$ is 1 (see Figure 19). In set notation, the unit circle can be written as

$$U = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

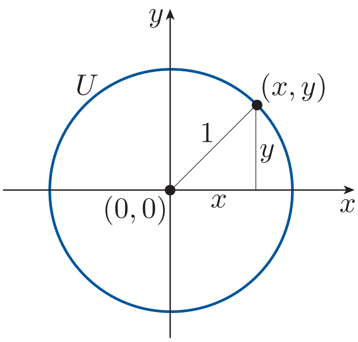


Figure 19 The unit circle U

Exercise A15

(a) Use set notation to specify the circle C of radius 3 centred at $(1,-4)$.

(b) Sketch the circle $C = \{(x,y) \in \mathbb{R}^2 : (x-1)^2 + (y-3)^2 = 4\}$.

Half-planes, discs and other plane sets

Consider the line

$$l = \{(x,y) \in \mathbb{R}^2 : y = 1 - x\}.$$

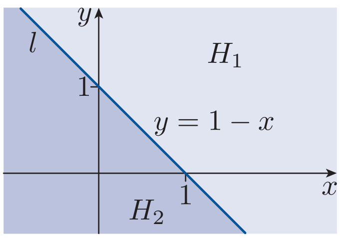


Figure 20 The plane split into three parts by l

This line splits $\mathbb{R}^2$ into three separate parts, as shown in Figure 20: the line l itself, the set H_1 of points lying *above* the line, and the set H_2 of points lying *below* the line.

For any point $P = (x,y)$ in H_1, the point $Q = (x, 1-x)$ lies on the line l, directly below P, as illustrated in Figure 21, so $y > 1 - x$. Similarly, each point (x,y) in H_2 satisfies $y < 1 - x$. Thus

$$H_1 = \{(x,y) \in \mathbb{R}^2 : y > 1 - x\}$$

and

$$H_2 = \{(x,y) \in \mathbb{R}^2 : y < 1 - x\}.$$

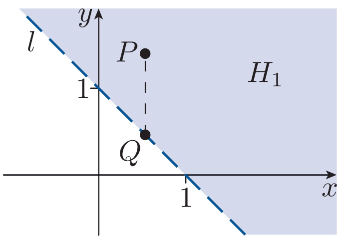


Figure 21 A point P in H_1

The set of points on one side of a line, possibly together with all the points on the line itself, is known as a **half-plane**. A half-plane that does not include the points on the line can be specified using set notation as in the examples H_1 and H_2 above. The corresponding half-plane that includes the points on the line can be specified by changing the symbol $>$ to $\geq$, or the symbol $<$ to $\leq$.

When we sketch a plane set that *excludes* a boundary line, as for the set H_1 in Figure 21, we draw the boundary as a *broken* line; if the plane set *includes* a boundary line, then we draw the boundary as a *solid* line.

We can treat other plane sets in a similar way. For example, consider the unit circle

$$U = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

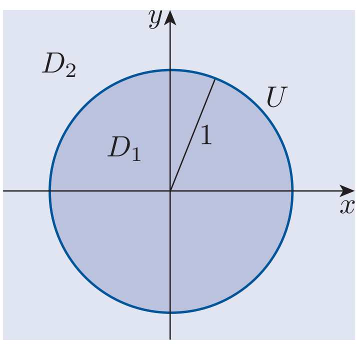


Figure 22 The plane split into three parts by the unit circle U

This circle splits $\mathbb{R}^2$ into three separate parts, as illustrated in Figure 22: the circle U itself, the set D_1 of points lying *inside* the circle and the set D_2 of points lying *outside* the circle.

The condition for a point (x,y) to lie inside U is that the distance of the point from the origin is less than 1. It follows that the square of the distance of the point (x,y) from the origin is also less than 1, so

$$D_1 = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}.$$

Similarly,

$$D_2 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 > 1\}.$$

The set of points inside a circle, possibly together with all the points on the circle, is known as a **disc**. Figure 23 shows the disc D_1 with the broken line indicating that the points on the circle are not included in the set.

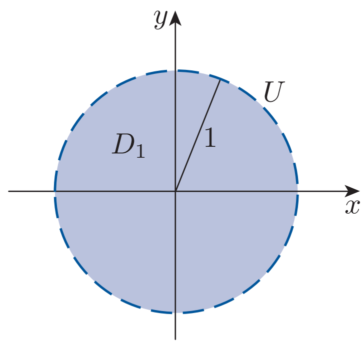


Figure 23 The disc D_1

If we wish to specify the disc consisting of the unit circle together with the points inside it, we replace the inequality $<$ by $\leq$ in the set notation specification of D_1 given above, and draw the boundary as a solid line.

As another example, consider the set of points lying inside the square with vertices $(0, 0)$, $(1, 0)$, $(1, 1)$ and $(0, 1)$, shown in Figure 24. This set can be written as

$$\{(x, y) \in \mathbb{R}^2 : 0 < x < 1,\ 0 < y < 1\}.$$

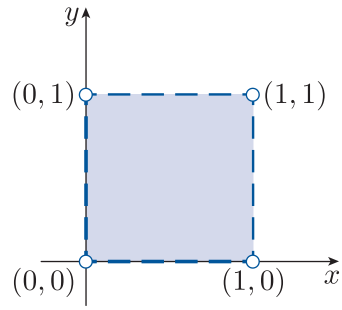


Figure 24 The points inside a square

The square boundary is excluded from this set, and we indicate this by drawing the boundary lines as broken lines and the vertices as *hollow* dots, as in Figure 24.

If we wish our set to include the square boundary, we replace each symbol $<$ by $\leq$, and we indicate this in a sketch by drawing the boundary lines as solid lines and the four vertices as *solid* dots.

These conventions for drawing plane sets are consistent with those you met earlier for intervals. They are summarised below.

Convention for drawing sets in $\mathbb{R}$ or $\mathbb{R}^2$

In a diagram of a subset of $\mathbb{R}$ or $\mathbb{R}^2$:

- included and excluded points are drawn as solid and hollow dots, respectively
- included and excluded boundaries are drawn as solid and broken lines, respectively.

Exercise A16

Sketch each of the following plane sets.

(a) $\{(x, y) \in \mathbb{R}^2 : x < 1\}$

(b) $\{(x, y) \in \mathbb{R}^2 : y \leq 2 - 2x\}$

(c) $\{(x, y) \in \mathbb{R}^2 : (x - 1)^2 + (y - 2)^2 < 4\}$

(d) $\{(x, y) \in \mathbb{R}^2 : x^2 + (y + 3)^2 > 1\}$

Exercise A17

Use set notation to specify the set of points inside the square with vertices $(0, 1)$, $(2, 1)$, $(2, 3)$, $(0, 3)$, together with the boundary, and sketch this set.

2.5 Set equality and subsets

Consider the sets $A = \{1, -1\}$ and $B = \{x \in \mathbb{R} : x^2 - 1 = 0\}$. Although these sets are written in different ways, each set contains exactly the same elements, 1 and -1. We say that these sets are *equal*.

Definition

Two sets A and B are **equal** if they have exactly the same elements; we write $A = B$.

When two sets each contain a small number of elements, we can usually check whether these elements are the same, and hence decide whether the sets are equal.

Exercise A18

Decide whether each of the following is a pair of equal sets.

(a) $A = \{2, -3\}$ and $B = \{x \in \mathbb{R} : x^2 + x - 6 = 0\}$.

(b) $A = \{k \in \mathbb{Z} : k \text{ is odd and } 0 < k < 8\}$ and
$B = \{2n + 1 : n \in \mathbb{N} \text{ and } n^2 < 25\}$.

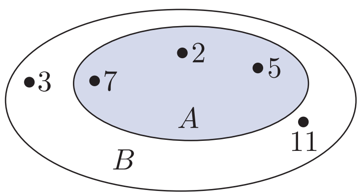


Figure 25 A subset A of a set B

If two sets each contain more than a small number of elements, it is less easy to check whether they are equal. You will meet a method for dealing with cases like this shortly, but first we need the following idea.

Consider the sets $A = \{7, 2, 5\}$ and $B = \{2, 3, 5, 7, 11\}$. These sets are illustrated in the Venn diagram in Figure 25. Each element of A is also an element of B. We say that A is a *subset* of B.

Definition

A set A is a **subset** of a set B if each element of A is also an element of B. We also say that A is *contained in* B, and we write $A \subseteq B$.

Do not confuse the symbol $\subseteq$ with the symbol $\in$. For example, we write

$$\{1\} \subseteq \{1, 2, 3\} \quad \text{and} \quad 1 \in \{1, 2, 3\},$$

because $\{1\}$ is a *subset* of $\{1,2,3\}$ and 1 is an *element* of $\{1,2,3\}$.

We sometimes indicate that a set A is a subset of a set B by reversing the symbol $\subseteq$ and writing $B \supseteq A$, which we read as 'B contains A'.

To indicate that A is *not* a subset of B, we write $A \not\subseteq B$. We may also write this as $B \not\supseteq A$, which we read as 'B does not contain A'.

The next box gives two simple but important facts about subsets.

Subsets of every set

For every set B:

- B is a subset of itself, that is $B \subseteq B$
- the empty set $\varnothing$ is a subset of B, that is, $\varnothing \subseteq B$.

The first result in the box follows immediately from the definition of a subset, given earlier. The second result in the box also follows from the definition, since any set B contains every element of the empty set, for the simple reason that the empty set has no elements.

When we wish to determine whether a set A is a subset of a set B, the method we use depends on the way in which the two sets are defined. If A has a small number of elements, then we can check individually whether each element of A is an element of B. Otherwise, we determine algebraically whether an arbitrary element of A fulfils the membership criteria for B, as illustrated in Worked Exercise A4 below.

To show that a set A is *not* a subset of a set B, we need to find at least one element of A that does not belong to B.

Worked Exercise A4

In each of the following cases, determine whether $A \subseteq B$.

(a) $A = \{1, 2, -4\}$ and $B = \{x \in \mathbb{R} : x^5 + 4x^4 - x - 4 = 0\}$.

(b) $A = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$ and $B = \{(x, y) \in \mathbb{R}^2 : x < 1\}$.

Solution

(a) A has only a few elements, so we can check individually whether they satisfy the membership criteria for B.

The elements 1, 2, -4 belong to $\mathbb{R}$, and

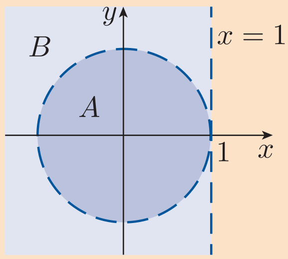
$$1^5 + 4 \times 1^4 - 1 - 4 = 0, \quad \text{so } 1 \in B,$$

$$2^5 + 4 \times 2^4 - 2 - 4 = 90, \quad \text{so } 2 \notin B.$$

Hence A is not a subset of B, that is, $A \nsubseteq B$.

(b) For plane sets, a sketch is often helpful.

The sets A and B are sketched below.



It appears that $A \subseteq B$ but we cannot check each element of A individually, so we try to prove this algebraically.

Let (x, y) be an arbitrary element of A; then (x, y) is a point in $\mathbb{R}^2$ with $x^2 + y^2 < 1$.

Since $y^2 \geq 0$, this implies that $x^2 < 1$, and hence that $x < 1$. Thus $(x, y) \in B$.

Since (x, y) is an arbitrary element of A, we conclude that A is a subset of B, that is, $A \subseteq B$.

Exercise A19

In each of the following cases, determine whether $A \subseteq B$.

(a) $A = \{(5, 2), (1, 1), (-3, 0)\}$ and $B = \{(x, y) \in \mathbb{R}^2 : x - 4y = -3\}$.

(b) $A = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$ and $B = \{(x, y) \in \mathbb{R}^2 : y < 0\}$.

(c) $A = [-1, 0]$ and $B = \{x \in \mathbb{R} : (x + 1)^2 \leq 1\}$.

If a set A is a subset of a set B that is not equal to B, then we say that A is a **proper subset** of B, and we write $A \subset B$ or $B \supset A$.

In some texts, the symbol $\subset$ is used to mean 'is a subset of' (for which we use the symbol $\subseteq$) rather than 'is a proper subset of'.

To show that a set A is a proper subset of a set B, we must show both that A is a subset of B, and that there is at least one element of B that is not an element of A.

Worked Exercise A5

Show that A is a proper subset of B, where:

$A = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$ and $B = \{(x, y) \in \mathbb{R}^2 : x < 1\}$.

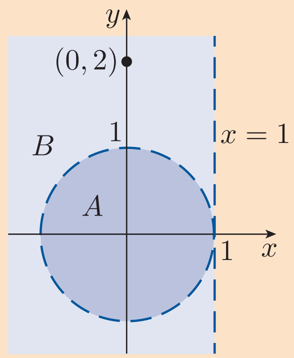
(A and B are the sets you met in Worked Exercise A4(b).)

Solution

We showed in the solution to Worked Exercise A4(b) that $A \subseteq B$.

A sketch can help us find a point in B but not in A. We must then confirm this algebraically.

The sets A and B are sketched below.



The point $(0, 2)$, for example, lies in B, since its x-coordinate 0 is less than 1, but $(0, 2)$ does not lie in A, since $0^2 + 2^2 = 4 \geq 1$. This shows that A is a proper subset of B; that is, $A \subset B$.

Exercise A20

In each of the following cases show that A is a proper subset of B.

(a) $A = \{(5, 2), (1, 1), (-3, 0)\}$ and $B = \{(x, y) \in \mathbb{R}^2 : x - 4y = -3\}$.

(b) $A = [-1, 0]$ and $B = \{x \in \mathbb{R} : (x + 1)^2 \leq 1\}$.

(These sets are the same as those in Exercise A19(a) and (c).)

We now return to the question of how we can show that two sets A and B are equal if they have more than a small number of elements.

If A is a subset of B, we have seen that A is either a *proper* subset of B or is equal to B. Similarly, if B is a subset of A, then B is either a proper subset of A or is equal to A. It follows that, if A is a subset of B *and* B is a subset of A, then the two sets A and B must be equal. This gives us our strategy.

Strategy A1

To show that the sets A and B are equal:

- first show that $A \subseteq B$
- then show that $B \subseteq A$.

Worked Exercise A6

Show that the following sets are equal:

$$A = \{(\cos t, \sin t) : t \in [0, 2\pi]\} \quad \text{and}$$
$$B = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

Solution

We could specify A by
$A = \{(x, y) \in \mathbb{R}^2 : x = \cos t,\ y = \sin t \text{ for some } t \in [0, 2\pi]\}$.

First we show that $A \subseteq B$.

Let (x, y) be an arbitrary element of A; then (x, y) is a point in $\mathbb{R}^2$.

We have $x = \cos t$ and $y = \sin t$, for some $t \in [0, 2\pi]$. So

$$x^2 + y^2 = \cos^2 t + \sin^2 t = 1.$$

This implies that $(x, y) \in B$, so $A \subseteq B$.

Next we show that $B \subseteq A$.

Let (x, y) be an arbitrary element of B; then

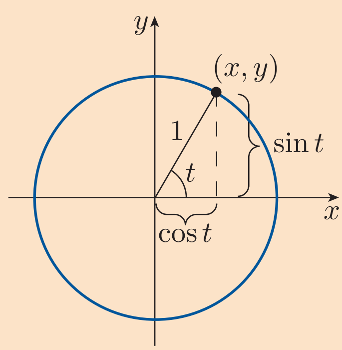
$$x^2 + y^2 = 1.$$

So (x, y) lies on the unit circle.

To show that (x, y) is an element of A, we need to find an angle $t \in [0, 2\pi]$ such that $(x, y) = (\cos t, \sin t)$. A sketch will help.

If we take t to be the (anticlockwise) angle from the (positive) x-axis to the line joining the point (x, y) with the origin, then $t \in [0, 2\pi]$, and

$$x = \cos t \quad \text{and} \quad y = \sin t.$$



It follows that $(x, y) \in A$, so $B \subseteq A$.

Since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$.

Exercise A21

In each of the following cases, show that the sets A and B are equal.

(a) $A = \{(t^2, 2t) : t \in \mathbb{R}\}$ and $B = \{(x, y) \in \mathbb{R}^2 : y^2 = 4x\}$.

(b) $A = \{(x, y) \in \mathbb{R}^2 : 2x + y - 3 = 0\}$ and $B = \{(t + 1, 1 - 2t) : t \in \mathbb{R}\}$.

2.6 Set operations

Consider the two sets $\{2, 3, 5\}$ and $\{1, 2, 5, 8\}$. Using these sets, we can construct several new sets – for example:

- the set $\{1, 2, 3, 5, 8\}$ consisting of all elements belonging to *at least one* of the two sets
- the set $\{2, 5\}$ consisting of all elements belonging to *both* of the two sets
- the set $\{3\}$ consisting of all elements belonging to the first set but not the second, and the set $\{1, 8\}$ consisting of all elements belonging to the second set but not the first.

Each of these new sets is a particular instance of a general construction for sets. We now consider them in turn.

Union

You saw above that if $A = \{2, 3, 5\}$ and $B = \{1, 2, 5, 8\}$, then the set of all elements belonging to at least one of the sets A and B is $\{1, 2, 3, 5, 8\}$. We call this set the *union* of A and B.

More generally, we have the following definition, which is illustrated by the Venn diagram in Figure 26.

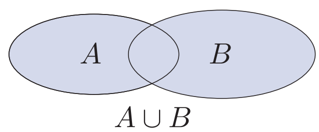


Figure 26 The union of sets A and B

Definition

Let A and B be any two sets; then the **union** of A and B is the set

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

The word *or* in this definition is used in the *inclusive* sense of 'and/or'; that is, the set $A \cup B$ consists of the elements of A and the elements of B, including the elements in both A and B. In everyday language, an example of 'or' used in the *exclusive* sense is 'Tea or coffee?', since the answer 'Both, please!' is not expected. An example of 'or' used in the *inclusive* sense is 'Milk or sugar?', since in this case you could answer 'Both'.

Worked Exercise A7

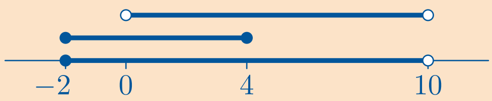
(a) Simplify $[-2,4] \cup (0,10)$.

(b) Sketch a diagram depicting the union of the half-plane H and the disc D, where

$$H = \{(x,y) \in \mathbb{R}^2 : y \leq 2 - 2x\},$$
$$D = \{(x,y) \in \mathbb{R}^2 : (x-1)^2 + (y-2)^2 < 4\}.$$

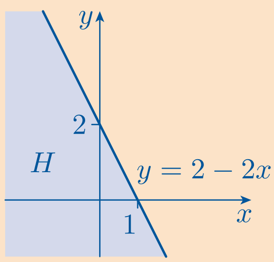
Solution

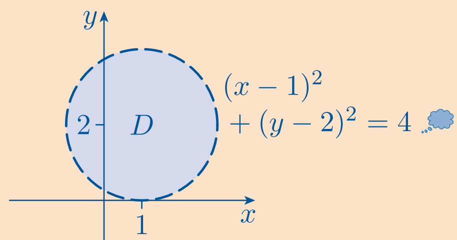
(a) These intervals overlap.



We have $[-2,4] \cup (0,10) = [-2,10)$.

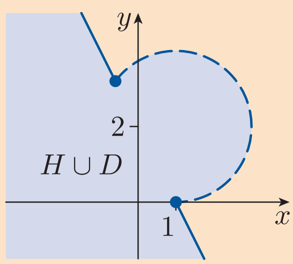
(b) These are the half-plane and disc from Exercise A16(b) and (c).





The union consists of all the points in H or D or both; the two points where the circle and line meet are both in the set H and so are both in the union $H \cup D$ and are shown as solid dots.

The set $H \cup D$ is as follows.



When sketching a set such as that in Worked Exercise A7(b), you should include enough detail so that the set is clear, and therefore the axes and an indication of scale are essential. Finding the exact points where the circle and line meet is not required, but can sometimes be helpful. In this case, substituting $y = 2 - 2x$ into the equation for the circle gives

$$(x-1)^2 + (-2x)^2 = 4,$$

which simplifies to

$$5x^2 - 2x - 3 = 0.$$

This factorises as

$$(x-1)(5x+3) = 0,$$

which has solutions $x = 1$ and $x = -\frac{3}{5}$, so the circle and line meet at the two points $(1, 0)$ and $\left(-\frac{3}{5}, 3\frac{1}{5}\right)$.

Exercise A22

(a) Simplify $(1, 7) \cup [4, 11]$.

(b) Express the set $\mathbb{R}^*$ as a union of intervals.

(c) Sketch a diagram depicting the union of the half-plane H and disc D, where

$$H = \{(x, y) \in \mathbb{R}^2 : y < 0\},$$
$$D = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \le 4\}.$$

So far you have seen the definition of the union of two sets. There is a similar definition for the union of any number of sets; for example, the union of three sets A, B and C, as illustrated by the Venn diagram in Figure 27, is the set

$$A \cup B \cup C = \{x : x \in A \text{ or } x \in B \text{ or } x \in C\}.$$

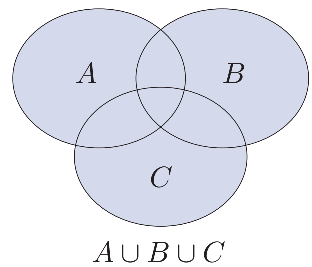


Figure 27 The union of sets A, B and C

Intersection

You saw above that if $A = \{2, 3, 5\}$ and $B = \{1, 2, 5, 8\}$, then the set of all elements belonging to both set A and set B is $\{2, 5\}$. We call this set the *intersection* of A and B.

More generally, we have the following definition, which is illustrated by the Venn diagram in Figure 28.

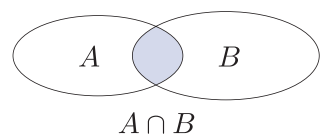


Figure 28 The intersection of sets A and B

Definition

Let A and B be any two sets; then the **intersection** of A and B is the set

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

Two sets with no element in common, such as $\{1,3,5\}$ and $\{2,9\}$, are said to be **disjoint**. We write this as $\{1,3,5\} \cap \{2,9\} = \varnothing$ since this intersection is empty.

Worked Exercise A8

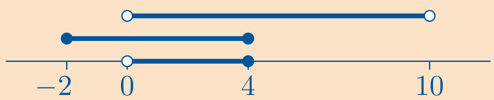
(a) Simplify $[-2,4] \cap (0,10)$.

(b) Sketch a diagram depicting the intersection of the half-plane H and disc D, where

$$H = \{(x,y) \in \mathbb{R}^2 : y \le 2 - 2x\},$$
$$D = \{(x,y) \in \mathbb{R}^2 : (x-1)^2 + (y-2)^2 < 4\}.$$

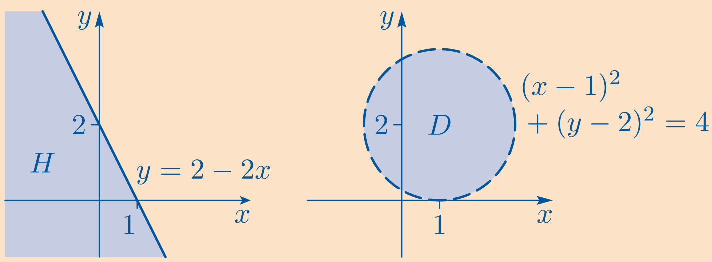
Solution

(a) The intersection is the overlap of these intervals.



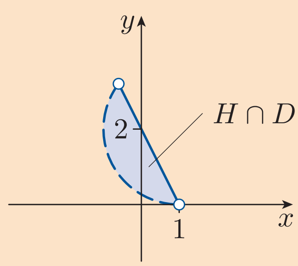
We have $[-2,4] \cap (0,10) = (0,4]$.

(b) These are the half-plane and disc from Exercise A16(b) and (c), and Worked Exercise A7.



The intersection consists of all the points in both H and D. Neither of the points where the circle and the line meet are in the set D, so these points are not in the intersection $H \cap D$, and both are shown as hollow dots.

The set $H \cap D$ is as follows.



Exercise A23

(a) Simplify $(1, 7) \cap [4, 11]$.

(b) Sketch a diagram depicting the intersection of the half-plane H and disc D, where

$$H = \{(x, y) \in \mathbb{R}^2 : y < 0\},$$
$$D = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}.$$

(These are the same sets as in Exercise A22(a) and (c).)

So far you have seen the definition of the intersection of two sets. There is a similar definition for the intersection of any number of sets; for example, the intersection of three sets A, B and C, as illustrated by the Venn diagram in Figure 29, is the set

$$A \cap B \cap C = \{x : x \in A \text{ and } x \in B \text{ and } x \in C\}.$$

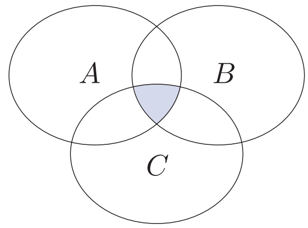


Figure 29 The intersection of sets A, B and C

Difference

You saw above that if $A = \{2, 3, 5\}$ and $B = \{1, 2, 5, 8\}$, then the set of all elements belonging to A but not to B is $\{3\}$; we call this set the *difference* $A - B$. Similarly, the set of all elements belonging to B but not to A is $\{1, 8\}$; this set is the *difference* $B - A$.

More generally, we have the following definition, which is illustrated by the Venn diagram in Figure 30.

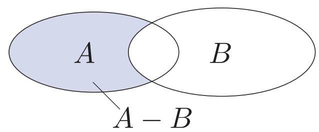


Figure 30 The difference between set A and set B

Definition

Let A and B be any two sets; then the **difference** between A and B is the set

$$A - B = \{x : x \in A,\ x \notin B\}.$$

Notice that $A - B$ is different from $B - A$ when $A \neq B$. This is unlike the union and intersection, where $A \cup B = B \cup A$ and $A \cap B = B \cap A$, for any sets A and B. Also, for any set A, we have $A - A = \varnothing$, again unlike the union and intersection, where $A \cup A = A \cap A = A$.

In some texts the difference $A - B$ of two sets A and B is denoted by $A \setminus B$.

Worked Exercise A9

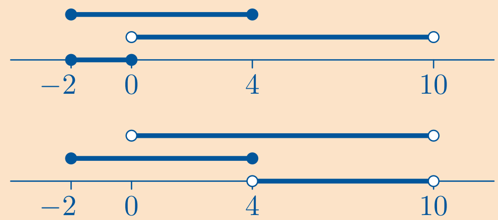
(a) Simplify $[-2, 4] - (0, 10)$ and $(0, 10) - [-2, 4]$.

(b) Sketch diagrams depicting the differences $H - D$ and $D - H$ of the half-plane H and disc D, where

$$H = \{(x, y) \in \mathbb{R}^2 : y \leq 2 - 2x\},$$
$$D = \{(x, y) \in \mathbb{R}^2 : (x-1)^2 + (y-2)^2 < 4\}.$$

Solution

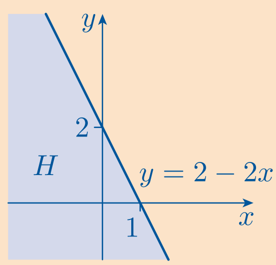
(a)

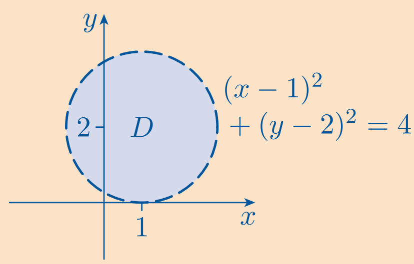


We have

$$[-2, 4] - (0, 10) = [-2, 0],$$
$$(0, 10) - [-2, 4] = (4, 10).$$

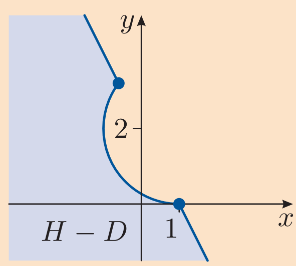
(b) Again these are the half-plane and disc from Exercise A16(b) and (c), and Worked Exercises A7 and A8.

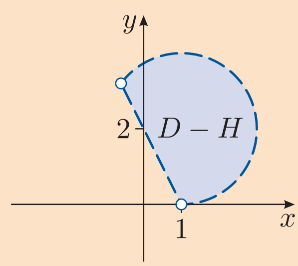




Consider carefully the boundary points, and in particular, the points where the line and circle meet. Both of the meeting points are in $H - D$, as are the remaining points of the boundaries. Neither of the meeting points is in the difference $D - H$, nor are the remaining points of the boundaries.

The sets $H - D$ and $D - H$ are as follows.





Exercise A24

(a) Simplify $(1,7) - [4,11]$ and $[4,11] - (1,7)$.

(b) Sketch diagrams depicting the differences $H - D$ and $D - H$ of the half-plane H and disc D, where

$$H = \{(x,y) \in \mathbb{R}^2 : y < 0\},$$
$$D = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}.$$

(These are the same sets as in Exercise A22(a) and (c), and Exercise A23.)

3 Functions

In this section you will revise what is meant by a *function*, and some associated ideas. You will look at not only functions of real numbers, but also functions of other mathematical objects. The idea of a function is fundamental throughout this module, so it is vital that you have a good understanding of this topic.

Gottfried Wilhelm Leibniz

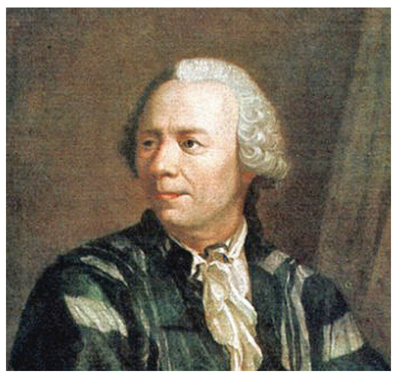
The term 'function' first emerged at the end of the seventeenth century in the correspondence of Gottfried Wilhelm Leibniz (1646–1716) and Johann Bernoulli (1667–1748). But it was Leonhard Euler (1707–1783) in the middle of the eighteenth century who was responsible for the essential development, notably through his *Introductio in Analysin Infinitorum* of 1748, the first work in which the concept of a function plays an explicit and central role.

Johann Bernoulli

3.1 What is a function?

You can think of a *function* as a machine for processing mathematical objects, such as numbers, points in the plane or vectors.

For example, consider the function f that takes non-zero real numbers as its inputs and whose rule is that the input x leads to the output $f(x) = 1/x$. You can regard it as a machine that calculates the reciprocals of its input numbers. When 3 is fed into the machine, out comes $\frac{1}{3}$; when -2 is fed into the machine, out comes $-\frac{1}{2}$; and so on. Any real number in the *domain* $\mathbb{R}^*$ of f can be processed by the machine to produce a real number in the *codomain* $\mathbb{R}$ of f, as illustrated in Figure 31.



Leonhard Euler

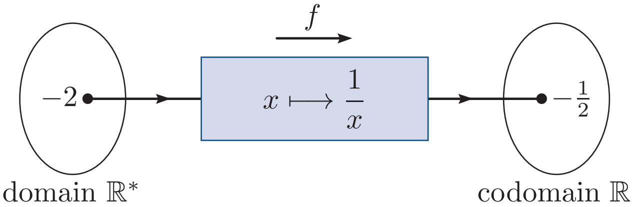


Figure 31 A function as a machine

Similarly, consider the function g that accepts points in the plane as its inputs and whose rule is that the input (x, y) leads to the output $g((x, y)) = y$. You can regard it as a machine that calculates the y-coordinate of each input point. When the point $(1, 2)$ is fed into the machine, out comes 2; when the point $(0, 0)$ is fed into the machine, out comes 0; and so on. Any point in the domain $\mathbb{R}^2$ of g can be processed by the machine to produce a real number in the codomain $\mathbb{R}$ of g, as illustrated in Figure 32.

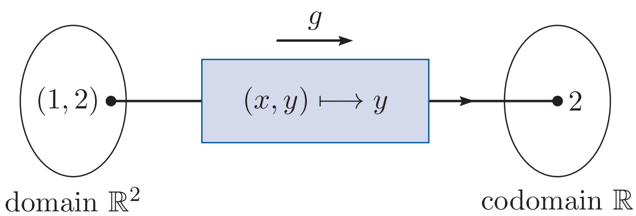


Figure 32 Another function as a machine

In general, imagine a machine that accepts an element x from some set A, and processes it to produce a single element $f(x)$ in some set B. This machine corresponds to the following general definition of a function, which is illustrated in Figure 33.

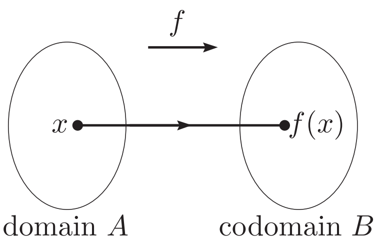


Figure 33 A general function

Definition

A **function** f is defined by specifying:

- a set A, called the **domain** of f
- a set B, called the **codomain** of f
- a **rule** $x \longmapsto f(x)$ that associates each element $x \in A$ with a unique element $f(x) \in B$.

The element $f(x)$ is the **image** of x under f.

Symbolically, we write

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longmapsto f(x). \end{aligned}$$

We often refer to a function as a **mapping**, and say that f **maps** A to B and x to $f(x)$.

Notice that the definition of a function does not require *every* element of the codomain B to be the image of an element of the domain A, but it *does* require every element of the domain A to have an image in the codomain B. For example, a function with rule $x \longmapsto \sin x$ and domain $\mathbb{R}$ could have codomain $\mathbb{R}$, or $[-1, 1]$, or any set of real numbers of which $[-1, 1]$ is a subset, but not, say, codomain $[0, 1]$ since the image of $3\pi/2$ is $\sin(3\pi/2) = -1$, which is not in this set.

Notice also that the symbolic definition of a function given at the end of the box above specifies all three of the constituent parts of a function at once: the domain, the codomain and the rule. For example, the definition

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ n &\longmapsto n + 1 \end{aligned}$$

specifies a function with domain $\mathbb{Z}$, codomain $\mathbb{Z}$ and rule $f(n) = n + 1$.

When we write a function symbolically, the first arrow is unbarred to signify a mapping from the domain A to the codomain B. The second arrow is barred, to show that the *particular* element x of A is mapped to the *particular* element $f(x)$ of B. Each arrow is read as 'maps to'.

The following paragraphs give a number of examples of different types of functions.

Real functions

A function whose domain and codomain are both subsets of $\mathbb{R}$ is called a **real function**. Examples include the functions

$$\begin{aligned} f : \mathbb{R}^* &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{x} \end{aligned} \qquad \text{and} \qquad \begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 2x - 5. \end{aligned}$$

In some texts, a real function is defined to be a function whose codomain is a subset of $\mathbb{R}$, but whose domain can be any set.

You may be more familiar with seeing these functions written as simply $f(x) = 1/x$ and $g(x) = 2x - 5$. We write functions in this shortened way when it is understood from the context what the domain and codomain are.

Distance function

Functions of the form $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ can be used to specify quantities associated with points in the plane. For example, the function

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto \sqrt{x^2 + y^2} \end{aligned}$$

gives the distance of each point (x, y) in the plane from the origin, as shown in Figure 34.

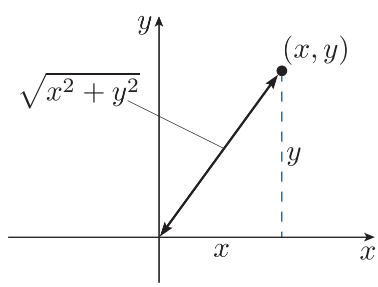


Figure 34 The distance of a point from the origin

Transformations of the plane

Functions that have a geometric interpretation are often called **transformations**. Such functions include translations, reflections and rotations of the plane. We now look at some simple examples. For each one, the diagram shows the effect of the transformation on the square whose vertices are at $(0,0)$, $(1,0)$, $(1,1)$ and $(0,1)$; part of the square is shaded for clarity.

- The transformation

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\longmapsto (x+2, y) \end{aligned}$$

  is the **translation** of the plane that shifts (or translates) each point to the right by 2 units, as illustrated in Figure 35.

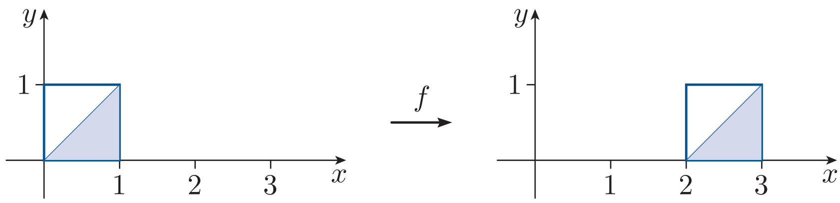


Figure 35 Translation 2 units to the right

- The transformation

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\longmapsto (-x, y) \end{aligned}$$

  is the **reflection** of the plane in the y-axis, as illustrated in Figure 36.

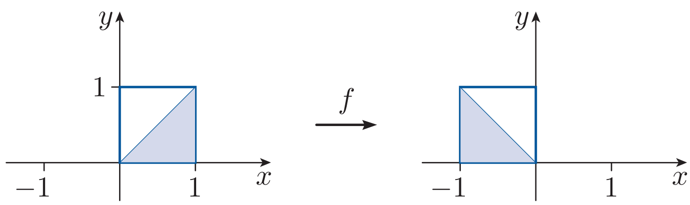


Figure 36 Reflection in the y-axis

- The transformation

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\longmapsto (-x, -y) \end{aligned}$$

  is the **rotation** of the plane through an angle π about the origin, as illustrated in Figure 37.

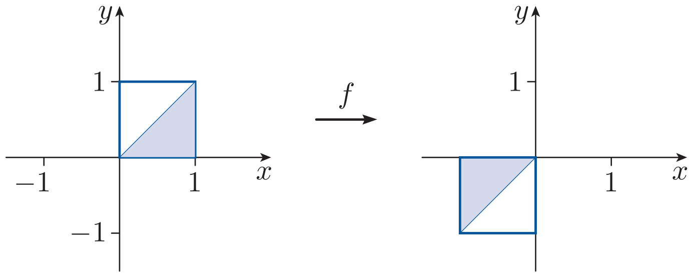


Figure 37 Rotation through an angle π about the origin

When specifying a function, like a transformation, where the elements of the domain are of the form (x, y), we simply write $f(x, y)$ rather than $f((x, y))$.

Exercise A25

For each of the following functions $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, state whether f is a translation, reflection or rotation of the plane.

(a) $f(x, y) = (x + 2, y + 3)$

(b) $f(x, y) = (x, -y)$

(c) $f(x, y) = (-y, x)$

Functions whose domains are finite sets

It is often useful to consider a function whose domain is a *finite* set. For example, we can define a function whose domain and codomain are the set

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

by

$$\begin{aligned} f : A &\longrightarrow A \\ x &\longmapsto 9 - x. \end{aligned}$$

When the domain of a function f has a small number of elements, we can specify the rule of f by listing the image $f(x)$ of each element x in the domain. For example, let $A = \{0, 1, 2, 3\}$ and $B = \{2, 3, 4, 5\}$; then we can define a function $f : A \longrightarrow B$ by the rule

$$f(0) = 2, \quad f(1) = 2, \quad f(2) = 4, \quad f(3) = 5.$$

We can represent the behaviour of this function by a diagram, as shown in Figure 38. A diagram of this type that represents a function always has the following features:

- there is *exactly one* arrow *from* each element in the domain, since each element in the domain has *exactly one* image in the codomain
- there may be no arrows, one arrow or several arrows going *to* an element in the codomain, since an element in the codomain may not be an image at all, may be an image of exactly one element in the domain, or may be an image of several elements in the domain.

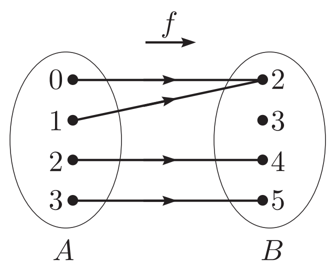
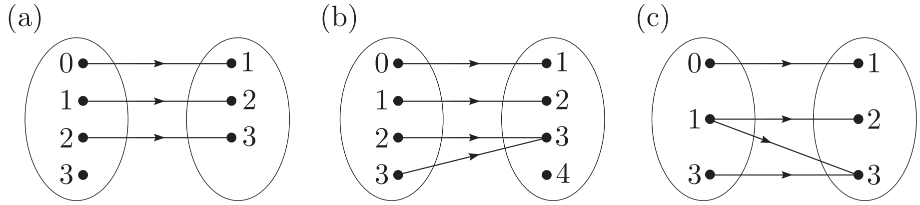


Figure 38 Function f from set A to set B

In the example shown in Figure 38, the number 3 is not an image at all, 5 is the image of 3 only, and 2 is the image of both 0 and 1.

Exercise A26

Which of the following diagrams represent(s) a function?



Identity functions

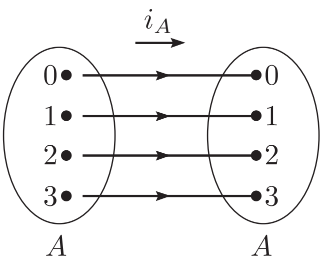


Figure 39 An identity function

Associated with any set A, there is a particularly simple function whose domain and codomain are the set A. This is the identity function i_A, which maps each element of A to itself. (We sometimes omit the subscript A if we do not need to emphasise the set.)

For example, let $A = \{0, 1, 2, 3\}$; then the rule of the identity function i_A, as illustrated in Figure 39, is

$$i_A(0) = 0, \quad i_A(1) = 1, \quad i_A(2) = 2, \quad i_A(3) = 3.$$

The following definition applies to *any* set A, finite or infinite.

Definition

The **identity function** on a set A is the function

$$\begin{aligned} i_A : A &\longrightarrow A \\ x &\longmapsto x. \end{aligned}$$

3.2 Image set of a function

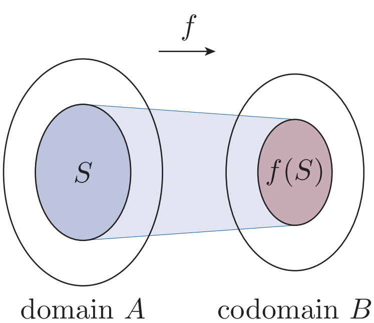


Figure 40 Image of a set S under a function f

The rule associated with a function tells us how to find the image of any element in the domain. Often, however, we need to consider the images of all elements in some subset of the domain. The subset of the codomain containing these images is called the *image* of the original subset, as stated below and illustrated in Figure 40.

Definition

Let $f : A \longrightarrow B$ be a function. For any subset S of A, the **image** of S under f, denoted by $f(S)$, is the set

$$f(S) = \{f(x) : x \in S\}.$$

Worked Exercise A10

Find $f(S)$, where $S = \{1, 2, 3\}$ and

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto \frac{1}{x}.$$

Solution

$f(S) = \{f(1), f(2), f(3)\} = \{1, \frac{1}{2}, \frac{1}{3}\}$.

Exercise A27

Let

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto x - 1.$$

Find the image under f of each of the following sets.

(a) $S = \{0, 1, 2, 3\}$ (b) $\mathbb{Z}$

The idea of the image of a subset of elements is useful in geometry, for example, where we frequently want to consider the effect of a transformation on a plane figure, a subset of $\mathbb{R}^2$. For example, suppose that S is the square with vertices at $(0, 0)$, $(1, 0)$, $(1, 1)$ and $(0, 1)$, and we want to find the image of S under the function

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$
$$(x, y) \longmapsto (x + 2, y).$$

This function is the translation of the plane that moves each point (x, y) to the right by 2. The image of S is therefore the square with vertices at $f(0, 0) = (2, 0)$, $f(1, 0) = (3, 0)$, $f(1, 1) = (3, 1)$ and $f(0, 1) = (2, 1)$, as shown in Figure 41.

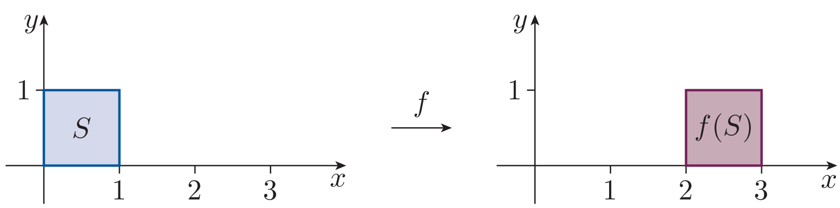


Figure 41 The image $f(S)$ of a square S under a translation f

Sometimes we want to consider the image of the *whole domain* of a function: this set is called the *image set* of the function, as illustrated in Figure 42.

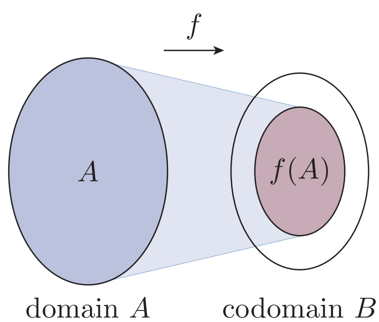


Figure 42 Image set of a function f

Definition

The **image set** of a function $f : A \longrightarrow B$ is the set

$$f(A) = \{f(x) : x \in A\}.$$

The image set of a function is a subset of its codomain. It need not be *equal* to the codomain because there may be some elements of the codomain that are not images of elements in the domain.

In some texts, the image set of a function is called the *image* of the function, or the *range* of the function.

When the domain of a function f has a small number of elements, we can find the image set of f by finding the image of each element in the domain, and listing them to form a set.

Worked Exercise A11

Let $A = \{-3, -2, -1, 0, 1, 2, 3\}$ and $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Find the image set of the function

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longmapsto x^2. \end{aligned}$$

Solution

The images of the elements of A are

$$f(-3) = 9, \quad f(-2) = 4, \quad f(-1) = 1, \quad f(0) = 0,$$
$$f(1) = 1, \quad f(2) = 4, \quad f(3) = 9.$$

So the image set of f is $f(A) = \{0, 1, 4, 9\}$.

Exercise A28

Let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Find the image set of the function

$$\begin{aligned} f : A &\longrightarrow A \\ x &\longmapsto 9 - x. \end{aligned}$$

You should have found that for the particular function in Exercise A28 the image set and the codomain are the same set. In other words, each element of the codomain is the image of an element in the domain, as illustrated in Figure 43. A function with this property is said to be *onto*.

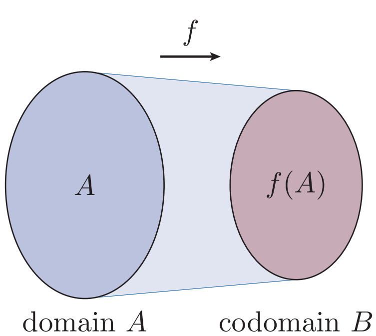


Figure 43 An onto function: $f(A) = B$

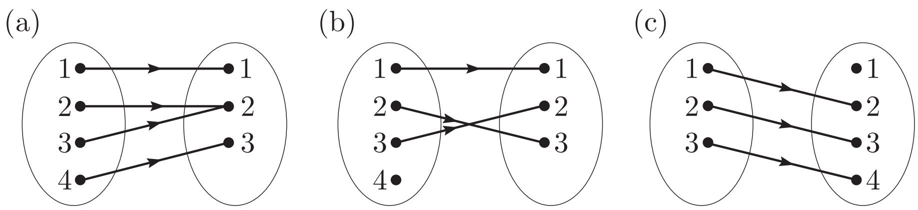
Definition

A function $f : A \longrightarrow B$ is **onto** if $f(A) = B$.

Some texts refer to an onto function as a *surjective* function.

Exercise A29

Which of the following diagrams represent(s) an onto function?



You have seen that if the domain of a function is a small finite set, then we can find the image set of the function by finding the image of each element of the domain individually. If the domain is a large finite set or an infinite set, then we need an algebraic argument to determine the image set. Sometimes we 'guess' what the image set seems to be, and then confirm this algebraically.

For a real function, a sketch of its graph can help us 'guess' the image set. For a function that is a transformation of the plane, we can use our knowledge of such transformations to help us 'guess' the image set.

To show that the image set is equal to our 'guess' set, we use our usual strategy for showing that two sets are equal: we show that each is a subset of the other.

- To show that the image set is a subset of our 'guess' set, we show that the image of an arbitrary element of the domain lies in our 'guess' set.
- To show that our 'guess' set is a subset of the image set, we take an arbitrary element of our 'guess' set and find an element of the domain whose image is this arbitrary element.

Worked Exercise A12

For each of the following functions, find its image set and determine whether it is onto.

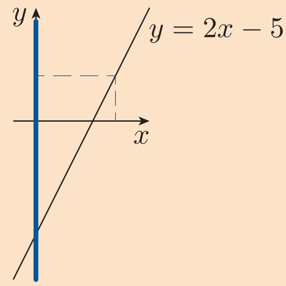
(a) $f : \mathbb{R} \longrightarrow \mathbb{R}$
$\quad x \longmapsto 2x - 5$

(b) $f : \mathbb{R} \longrightarrow \mathbb{R}$
$\quad x \longmapsto x^2$

(c) $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$
$\quad (x, y) \longmapsto (x + 1, y + 2)$

Solution

(a) A sketch of the graph of f is shown below.



For every element on the y-axis, a horizontal line drawn through that element meets the graph. So it seems that every element of the codomain is the image of some element of the domain. That is, we 'guess' that the image set $f(\mathbb{R})$ is the whole codomain $\mathbb{R}$.

We prove that $f(\mathbb{R}) = \mathbb{R}$.

The image set is always a subset of the codomain; in this case the codomain is $\mathbb{R}$, so $f(\mathbb{R}) \subseteq \mathbb{R}$.

We know that $f(\mathbb{R}) \subseteq \mathbb{R}$, so we must show that $f(\mathbb{R}) \supseteq \mathbb{R}$.

We take an arbitrary element in our 'guess' set $\mathbb{R}$, and find an element in the domain $\mathbb{R}$ whose image is this arbitrary element.

Let y be an arbitrary element in $\mathbb{R}$. We must show that $y \in f(\mathbb{R})$; that is, there exists an element x in the domain $\mathbb{R}$ such that

$$f(x) = y; \quad \text{that is,} \quad 2x - 5 = y.$$

Rearranging this equation, we obtain

$$x = \frac{y+5}{2}$$

which is in the domain $\mathbb{R}$. So we have

$$\begin{aligned} f(x) &= 2x - 5 \\ &= 2\left(\frac{y+5}{2}\right) - 5 \\ &= y, \end{aligned}$$

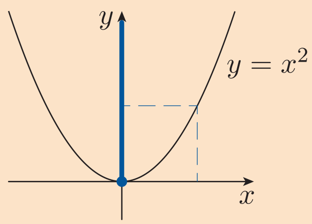
that is, for every $y \in \mathbb{R}$ there is an x in the domain $\mathbb{R}$ such that $f(x) = y$.

Thus $f(\mathbb{R}) \supseteq \mathbb{R}$.

Since $f(\mathbb{R}) \subseteq \mathbb{R}$ and $f(\mathbb{R}) \supseteq \mathbb{R}$, it follows that $f(\mathbb{R}) = \mathbb{R}$, so the image set of f is indeed $\mathbb{R}$.

The codomain of f is also $\mathbb{R}$, so f is onto.

(b) A sketch of the graph of f is shown below.



For every element in the interval $[0, \infty)$ of the y-axis (marked on the sketch), a horizontal line drawn through that element meets the graph. For any element outside this interval, such a horizontal line does not meet the graph. So we 'guess' that the image set $f(\mathbb{R})$ is $[0, \infty)$.

We prove that $f(\mathbb{R}) = [0, \infty)$.

We know that the image set is a subset of the codomain $\mathbb{R}$, but we don't know that it is a subset of $[0, \infty)$. We have to show algebraically that $f(\mathbb{R}) \subseteq [0, \infty)$ by finding the image of an arbitrary element in the domain $\mathbb{R}$.

Let x be an arbitrary element in the domain $\mathbb{R}$; then $f(x) = x^2$. Now, $x^2 \geq 0$ for all $x \in \mathbb{R}$, so $f(\mathbb{R}) \subseteq [0, \infty)$.

We must now show that $f(\mathbb{R}) \supseteq [0, \infty)$.

We take an arbitrary element in our 'guess' set $[0, \infty)$, and find an element of the domain $\mathbb{R}$ whose image is this arbitrary element.

Let y be an arbitrary element in $[0, \infty)$. We must show that there exists an element x in the domain $\mathbb{R}$ such that

$$f(x) = y; \quad \text{that is,} \quad x^2 = y.$$

Now $x = \sqrt{y}$ is in $\mathbb{R}$ (since $y \geq 0$) and satisfies $f(x) = y$, as required. Thus $f(\mathbb{R}) \supseteq [0, \infty)$.

Since $f(\mathbb{R}) \subseteq [0, \infty)$ and $f(\mathbb{R}) \supseteq [0, \infty)$, it follows that $f(\mathbb{R}) = [0, \infty)$, so the image set of f is $[0, \infty)$.

The image set $f(\mathbb{R}) = [0, \infty)$ is not the whole of the codomain $\mathbb{R}$, so f is not onto.

If we had simply been asked to determine whether f is onto, we could have shown that it is not by finding just one element, say -1, in the codomain $\mathbb{R}$ that is not the image of an element of the domain $\mathbb{R}$.

(c) This function is a translation of the plane (it shifts each point to the right by 1 unit and up by 2 units). So we expect ('guess') the image set to be the plane $\mathbb{R}^2$.

We prove that $f(\mathbb{R}^2) = \mathbb{R}^2$.

The image set is always a subset of the codomain; in this case the codomain is $\mathbb{R}^2$, so $f(\mathbb{R}^2) \subseteq \mathbb{R}^2$.

We know that $f(\mathbb{R}^2) \subseteq \mathbb{R}^2$, so we must show that $f(\mathbb{R}^2) \supseteq \mathbb{R}^2$.

Let (x', y') be an arbitrary element in the codomain $\mathbb{R}^2$. We must show that there exists an element (x, y) in the domain $\mathbb{R}^2$ such that

$$f(x, y) = (x', y'); \quad \text{so,} \quad (x + 1, y + 2) = (x', y'),$$

that is, $x + 1 = x'$ and $y + 2 = y'$. Rearranging these two equations, we obtain

$$x = x' - 1, \quad y = y' - 2.$$

So, $(x, y) \in \mathbb{R}^2$ and $f(x, y) = (x', y')$, as required. Thus $f(\mathbb{R}^2) \supseteq \mathbb{R}^2$.

Since $f(\mathbb{R}^2) \subseteq \mathbb{R}^2$ and $f(\mathbb{R}^2) \supseteq \mathbb{R}^2$, it follows that $f(\mathbb{R}^2) = \mathbb{R}^2$, so the image set of f is $\mathbb{R}^2$.

The codomain of f is also $\mathbb{R}^2$, so f is onto.

Exercise A30

For each of the following functions, find its image set and determine whether it is onto.

(a) $\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 1 + x^2 \end{aligned}$ (b) $\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x, -y) \end{aligned}$

As you have seen from Worked Exercise A12 and Exercise A30, when you want to determine whether a function is onto, it is crucial to take into account what the *codomain* of the function is. For example, you saw in Worked Exercise A12 that the function

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned}$$

is not onto. To see this, you just have to observe that the element -1, for example, of the codomain is not the image of any element of the domain. However, if you remove all the negative numbers from the codomain of this function, then you obtain the new function

$$\begin{aligned} g : \mathbb{R} &\longrightarrow [0, \infty) \\ x &\longmapsto x^2, \end{aligned}$$

which is onto, since every element of the codomain is an image of an element of the domain. Note that these functions f and g are *different* functions, since they have different codomains.

3.3 Inverse functions

Given a function

$$f : A \longrightarrow B$$
$$x \longmapsto f(x),$$

it is sometimes possible to define an *inverse function* that 'undoes' the effect of f by mapping each image element $f(x)$ back to the element x whose image it is. For example, a rotation in the plane can be 'undone' by a rotation in the opposite direction.

However, consider the function

$$f : A \longrightarrow B$$
$$x \longmapsto x^2,$$

where $A = \{-3, -2, -1, 0, 1, 2, 3\}$ and $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

We know that $f(-2) = f(2) = 4$, and so a function that 'undoes' the effect of f must map the number 4 to the number -2 *and* to the number 2, which is impossible. Thus, in this case, no inverse function exists. This function f is an example of a function that is *many-to-one*. A many-to-one function does not have an inverse function.

Definitions

A function $f : A \longrightarrow B$ is **one-to-one** if each element of $f(A)$ is the image of exactly one element of A; that is,

$$\text{if } x_1, x_2 \in A \text{ and } f(x_1) = f(x_2), \quad \text{then } x_1 = x_2.$$

A function that is not one-to-one is **many-to-one**.

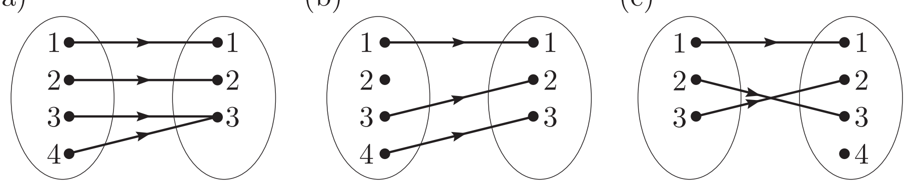
Thus a function f is one-to-one if it maps distinct elements in the domain A to distinct elements in the image set $f(A)$. Some texts refer to a one-to-one function as an *injective* function.

To prove that a function f is *not* one-to-one (that is, that the function is many-to-one), it is sufficient to find just one pair of *distinct* elements in the domain A with the *same* image under f.

Exercise A31

Which of the following diagrams represent(s) a one-to-one function?

(a) (b) (c)



If the domain of a function is a large finite set or an infinite set, then to show that the function is one-to-one, we need an algebraic argument. We aim to show algebraically that, if two elements of the domain have the same image under the function, then they must actually be the same element, as demonstrated in Worked Exercise A13.

Showing that a function is *not* one-to-one is more straightforward: we just give a pair of distinct elements that have the same image under the function, as you have seen.

For a real function, an initial sketch of its graph can help us 'guess' whether or not the function is one-to-one, and if it is not one-to-one, the graph can also help us find a pair of elements that show this.

Worked Exercise A13

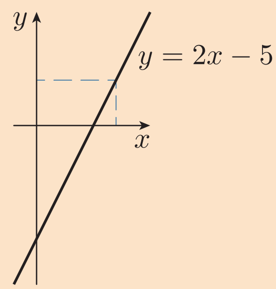
Determine which of the following functions are one-to-one.

(a) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto 2x - 5$ (b) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto x^2$ (c) $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(x, y) \longmapsto (x + 1, y + 2)$

(These are the same functions as in Worked Exercise A12.)

Solution

(a) A sketch of the graph of f is shown below.



Each horizontal line meets the graph just once. So it seems that no element of the codomain is the image of more than one element of the domain. That is, it seems that f is one-to-one. To prove this, we show that if two elements x_1 and x_2 in the domain have the same image, then they must actually be the *same* element.

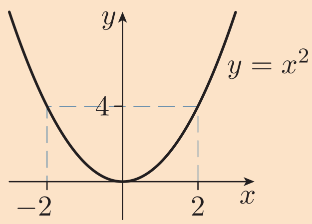
We show that f is one-to-one. Suppose that $f(x_1) = f(x_2)$; then

$$2x_1 - 5 = 2x_2 - 5,$$

so $2x_1 = 2x_2$, and hence $x_1 = x_2$.

Thus f is one-to-one.

(b) A sketch of the graph of f is shown below.



Some horizontal lines meet the graph more than once. So it seems that f is not one-to-one. To show this, we find two distinct elements of the domain with the same image.

This function is not one-to-one since, for example,

$$f(2) = f(-2) = 4.$$

(c) This function is a translation of the plane, so we expect it to be one-to-one.

We show that f is one-to-one. Suppose that $f(x_1, y_1) = f(x_2, y_2)$; then

$$(x_1 + 1, y_1 + 2) = (x_2 + 1, y_2 + 2).$$

Thus

$$x_1 + 1 = x_2 + 1 \quad \text{and} \quad y_1 + 2 = y_2 + 2,$$

so

$$x_1 = x_2 \quad \text{and} \quad y_1 = y_2.$$

Hence $(x_1, y_1) = (x_2, y_2)$, so f is one-to-one.

Exercise A32

Determine which of the following functions is one-to-one.

(a) $f : \mathbb{R} \longrightarrow \mathbb{R}$
$x \longmapsto 1 + x^2$

(b) $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$
$(x, y) \longmapsto (x, -y)$

(These are the same functions as in Exercise A30.)

For a one-to-one function $f : A \longrightarrow B$, we have the situation illustrated in Figure 44. Each element y in $f(A)$ is the image of a unique element x in A, and so we can reverse the arrows to obtain the *inverse function* with domain $f(A)$ and image set A, which maps y back to x. When it exists, we denote the inverse function of f by f^{-1}.

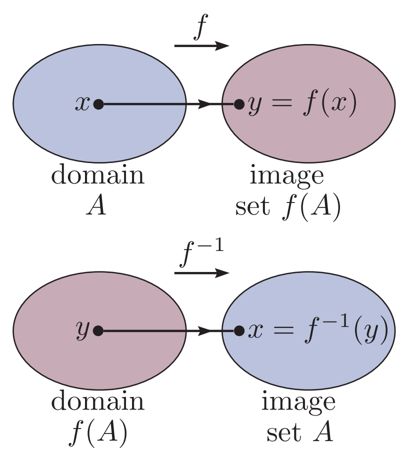


Figure 44 A function and its inverse

Definition

Let $f : A \longrightarrow B$ be a one-to-one function. Then f has an **inverse function** $f^{-1} : f(A) \longrightarrow A$, with rule

$$f^{-1}(y) = x, \quad \text{where } y = f(x).$$

Notice in this definition that the domain of f^{-1} is $f(A)$; it is not necessarily the whole of B.

However, if a function $f : A \longrightarrow B$ is *onto*, as well as one-to-one, then f has an inverse function $f^{-1} : B \longrightarrow A$; that is, the domain of f^{-1} *is* the whole of B.

A function $f : A \longrightarrow B$ that is both one-to-one and onto is said to be a **one-to-one correspondence** between the sets A and B. For such a function f, not only is f^{-1} the inverse of f, but also f is the inverse of f^{-1}; that is, the functions f and f^{-1} are inverses of each other.

Some texts refer to a one-to-one correspondence as a *bijection*.

Worked Exercise A14

For each of the following functions, determine whether f has an inverse function f^{-1}; if it exists, find it.

(a) $f : \mathbb{R} \longrightarrow \mathbb{R}$
$\quad x \longmapsto 2x - 5$

(b) $f : \mathbb{R} \longrightarrow \mathbb{R}$
$\quad x \longmapsto x^2$

(c) $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$
$\quad (x, y) \longmapsto (x + 1, y + 2)$

(d) $f : [0, \infty) \longrightarrow [-1, \infty)$
$\quad x \longmapsto 3x^2 - 1$

Solution

(a) In Worked Exercise A13(a), we showed that f is one-to-one, so f has an inverse function.

In Worked Exercise A12(a), we showed that the image set of f is $\mathbb{R}$ and that, for each y in the image set $\mathbb{R}$, there is an $x \in \mathbb{R}$ such that

$$y = f(x) = f\left(\frac{y+5}{2}\right).$$

Under f, we know that y is the image of $(y + 5)/2$, so under the inverse, $(y + 5)/2$ is the image of y.

So f^{-1} is the function

$$f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$$
$$y \longmapsto \frac{y+5}{2}.$$

It does not matter whether the definition of f^{-1} is expressed in terms of x or y, but it is more usual to use x in the definition of a real function.

This definition can be expressed in terms of x as

$$\begin{aligned} f^{-1} &: \mathbb{R} \longrightarrow \mathbb{R} \\ &x \longmapsto \frac{x+5}{2}. \end{aligned}$$

(b) In Worked Exercise A13(b), we showed that f is not one-to-one, so f does not have an inverse function.

(c) In Worked Exercise A13(c), we showed that f is one-to-one, so f has an inverse function.

In Worked Exercise A12(c), we showed that the image set of f is $\mathbb{R}^2$ and that, for each (x', y') in the image set $\mathbb{R}^2$, we have

$$(x', y') = f(x, y) = f(x' - 1, y' - 2).$$

Under f, we know that (x', y') is the image of $(x' - 1, y' - 2)$, so under the inverse, $(x' - 1, y' - 2)$ is the image of (x', y').

So f^{-1} is the function

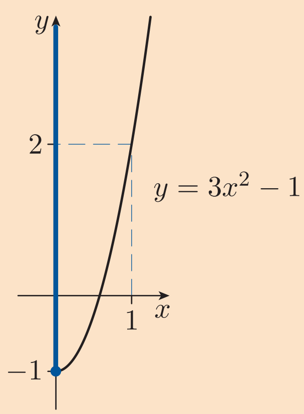
$$\begin{aligned} f^{-1} &: \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ &(x', y') \longmapsto (x' - 1, y' - 2). \end{aligned}$$

This definition can be expressed in terms of x and y as

$$\begin{aligned} f^{-1} &: \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ &(x, y) \longmapsto (x - 1, y - 2). \end{aligned}$$

This makes sense: geometrically, f is the translation that shifts each point to the right by 1 unit and up by 2 units, so we expect the inverse to be a translation to the left by 1 unit and down by 2 units.

(d) A sketch of the graph of f is shown below.



Each horizontal line meets the graph just once. So it seems that f is one-to-one. To prove this, we show that if two elements x_1 and x_2 in the domain have the same image, then they must actually be the *same* element.

We show that f is one-to-one. Suppose that $f(x_1) = f(x_2)$; then

$$3x_1^2 - 1 = 3x_2^2 - 1,$$

so $3x_1^2 = 3x_2^2$, and hence $x_1^2 = x_2^2$. Since both x_1 and x_2 are in the domain $[0, \infty)$, this implies that $x_1 = x_2$.

Thus f is one-to-one.

We now find the image set of f. From the sketch, we 'guess' that it is $[-1, \infty)$, the codomain of f. That is, we guess that f is onto.

We prove that $f([0, \infty)) = [-1, \infty)$.

The image set is a subset of the codomain.

We know that $f([0, \infty)) \subseteq [-1, \infty)$, so we must show that $f([0, \infty)) \supseteq [-1, \infty)$.

We take an arbitrary element in our 'guess' set $[-1, \infty)$, and find an element of the domain $[0, \infty)$ whose image is this arbitrary element.

Let y be an arbitrary element in $[-1, \infty)$. We must show that there exists an element x in the domain $[0, \infty)$ such that

$$f(x) = y; \quad \text{that is,} \quad 3x^2 - 1 = y.$$

Rearranging this equation, we obtain

$$x^2 = \frac{y+1}{3}.$$

Since $y \in [-1, \infty)$, we know $y + 1 \geq 0$, so

$$x = \sqrt{\frac{y+1}{3}}$$

is in the domain $[0, \infty)$. So we have

$$\begin{aligned} f(x) &= 3x^2 - 1 \\ &= 3\left(\sqrt{\frac{y+1}{3}}\right)^2 - 1 \\ &= \frac{3(y+1)}{3} - 1 \\ &= (y+1) - 1 \\ &= y, \end{aligned}$$

that is, for every $y \in [-1, \infty)$ there is an $x \in [0, \infty)$ such that $f(x) = y$.

Thus $f([0,\infty)) \supseteq [-1,\infty)$.

Since $f([0,\infty)) \subseteq [-1,\infty)$ and $f([0,\infty)) \supseteq [-1,\infty)$, it follows that $f([0,\infty)) = [-1,\infty)$, so the image set of f is indeed $[-1,\infty)$.

The image set of f is equal to the codomain, so f is onto.

Under f, we know that y is the image of $\sqrt{(y+1)/3}$, so under the inverse, $\sqrt{(y+1)/3}$ is the image of y.

So f^{-1} is the function

$$\begin{aligned} f^{-1} : [-1,\infty) &\longrightarrow [0,\infty) \\ y &\longmapsto \sqrt{(y+1)/3}. \end{aligned}$$

This can be expressed in terms of x as

$$\begin{aligned} f^{-1} : [-1,\infty) &\longrightarrow [0,\infty) \\ x &\longmapsto \sqrt{(x+1)/3}. \end{aligned}$$

Exercise A33

For each of the following functions, determine whether f has an inverse function f^{-1} and, if it exists, find it.

(a) $\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 1 + x^2 \end{aligned}$ (b) $\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\longmapsto (x,-y) \end{aligned}$ (c) $\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 8x + 3 \end{aligned}$

(For parts (a) and (b), use your answers from Exercises A30 and A32.)

Restrictions

When we are working with a function $f : A \longrightarrow B$, it is sometimes convenient to restrict attention to the behaviour of f on some subset C of A. For example, consider the function

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2. \end{aligned}$$

This function is not one-to-one and so does not have an inverse function. However, if the domain of f is replaced by the set $C = [0,\infty)$, then we obtain a related function,

$$\begin{aligned} g : C &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2, \end{aligned}$$

shown in Figure 45. The rule is the same as for f, but the domain is 'restricted' to produce a new function g that is one-to-one and so has an inverse.

The function g is an example of a *restriction* of f in the sense that $g(x) = f(x)$ for all x in the domain of g.

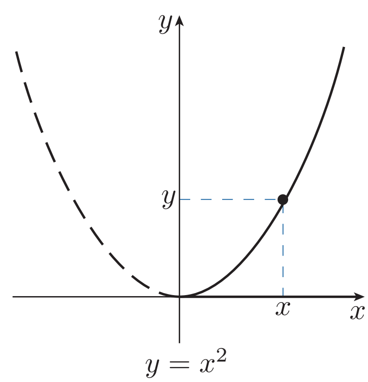


Figure 45 The function g with domain $[0,\infty)$

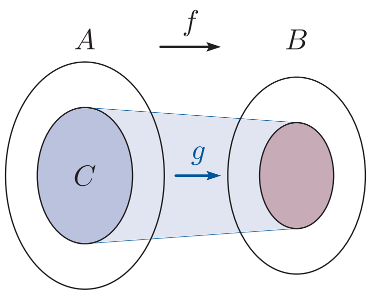


Figure 46 The function g is the restriction of f to C

More generally, we define a restriction, illustrated in Figure 46, as follows.

Definition

Let $f : A \longrightarrow B$ and let C be a subset of the domain A. Then the function $g : C \longrightarrow B$ defined by

$$g(x) = f(x), \quad \text{for } x \in C,$$

is the **restriction** of f to C.

Exercise A34

Let f be the function

$$\begin{aligned} f : \mathbb{R} &\longrightarrow [-1, 1] \\ x &\longmapsto \sin x. \end{aligned}$$

Write down a restriction of f that is one-to-one.

3.4 Composite functions

In Subsection 3.1, you saw how a function may be regarded as a machine that processes elements in the domain to produce elements in the codomain. Now suppose that two such machines are linked together, so that the elements emerging from the first machine are fed into the second machine for further processing. The overall effect is to create a new 'composite' machine that corresponds to a so-called *composite* function.

For example, consider the real functions

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned} \qquad \text{and} \qquad \begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 2x - 5. \end{aligned}$$

When the machines for f and g are linked together so that elements are first processed by f and then by g, we obtain the 'composite' machine illustrated by the large box in Figure 47.

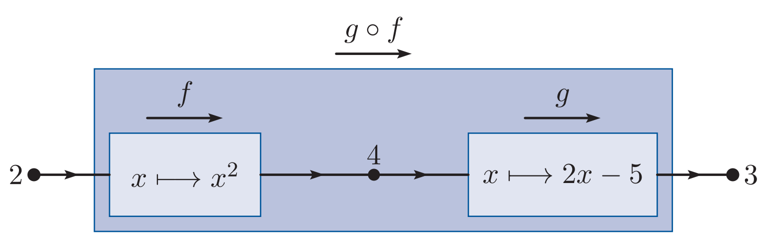


Figure 47 The composite function $g \circ f$ as a machine

For instance, when 2 is fed into the machine, it is first squared by f to produce the number 4, and then 4 is processed by g to give the number $(2 \times 4) - 5 = 3$.

Similarly, when an arbitrary real number x is fed into the machine, it is first processed by f to give the real number x^2. Since x^2 lies in $\mathbb{R}$, the domain of g, the number x^2 can then be processed by g to give $2x^2 - 5$. Thus, overall, the composite machine corresponds to a function, which we denote by $g \circ f$, whose rule is

$$(g \circ f)(x) = g(f(x)) = g(x^2) = 2x^2 - 5.$$

In general, we have the following definition.

Definition

Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be two functions such that the domain of g is the same set as the codomain, B, of f. Then the **composite function** $g \circ f$ is given by

$$\begin{aligned} g \circ f : A &\longrightarrow C \\ x &\longmapsto g(f(x)). \end{aligned}$$

Notice that $g \circ f$ means f first, then g.

Exercise A35

Let f and g be the functions

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto -x \end{aligned} \quad \text{and} \quad \begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 3x + 1. \end{aligned}$$

Determine the composite functions

(a) $g \circ f$, (b) $f \circ g$.

In general, the composite functions $g \circ f$ and $f \circ g$ are not equal, as you saw in Exercise A35.

Composite functions have many uses in mathematics; for example, we can use them to examine the effect of one transformation of the plane followed by another.

Suppose, for instance, that f and g are the reflections of the plane in the x-axis and y-axis respectively:

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x, -y) \end{aligned} \quad \text{and} \quad \begin{aligned} g : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (-x, y). \end{aligned}$$

The composite function $g \circ f$ describes the overall effect of first reflecting in the x-axis (changing the sign of y) and then reflecting in the y-axis (changing the sign of x), as shown in Figure 48. The rule of $g \circ f$ is

$$\begin{aligned} (g \circ f)(x, y) = g(f(x, y)) &= g(x, -y) \\ &= (-x, -y). \end{aligned}$$

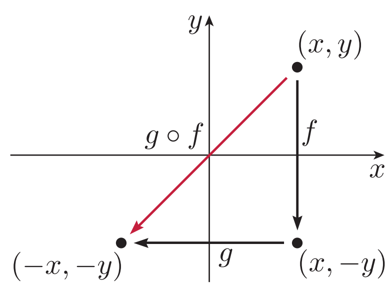


Figure 48 The composite $g \circ f$

Thus $g \circ f$ is the function

$$\begin{aligned} g \circ f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (-x, -y), \end{aligned}$$

which rotates the plane through an angle π about the origin, as can be seen by considering Figure 49, which shows how a square is transformed by $g \circ f$.

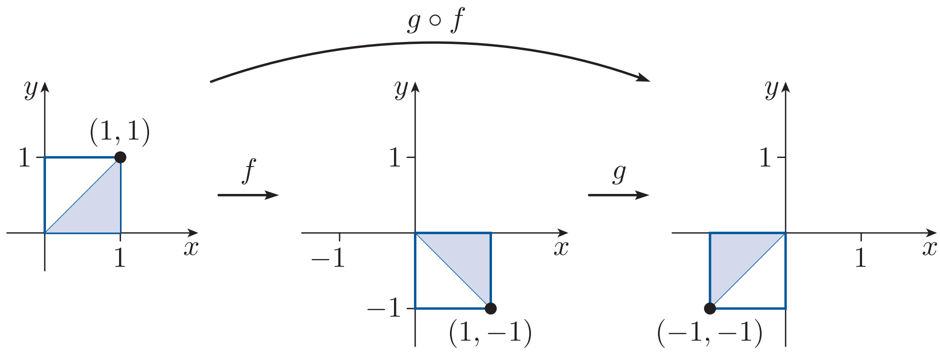


Figure 49 The composite function $g \circ f$ transforming a square

Exercise A36

Determine the composite function $f \circ g$, where f and g are the reflections of the plane in the x-axis and y-axis respectively, as defined above.

So far, we have considered the composite function $g \circ f$ only when the domain of the function g is the same as the codomain of the function f. We can, however, form the composite function $g \circ f$ when g and f are *any* two functions.

For example, consider the functions

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned} \quad \text{and} \quad \begin{aligned} g : \mathbb{R} - \{1\} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{x-1}. \end{aligned}$$

Recall that $\mathbb{R} - \{1\}$ is the set of all real numbers with 1 excluded.

Here the domain of g is not equal to the codomain of f, but we can still consider the composite function $g \circ f$, with the rule

$$(g \circ f)(x) = g(f(x)) = g(x^2) = \frac{1}{x^2 - 1}.$$

However, we have to be careful about the domain of $g \circ f$. It cannot be the whole of $\mathbb{R}$, the domain of f. To see this, consider what happens when we try to feed the number 1 into the 'machine' corresponding to $g \circ f$, as shown in Figure 50.

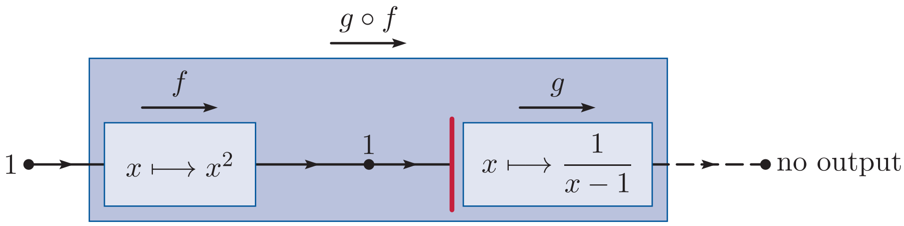


Figure 50 An input number that cannot be 'processed' by $g \circ f$

If we try to feed the number 1 into the machine, then it can be processed by f to produce the number 1, but 1 cannot then be processed by g, since it is not in the domain of g. We have the same problem if we try to feed the number -1 into the machine. However, if we feed any other number in the domain of f into the machine, then it can be processed by f and then g to produce a final output number. So we take the domain of $g \circ f$ to be $\mathbb{R} - \{1, -1\}$. Thus the composite function $g \circ f$ is

$$\begin{aligned} g \circ f : \mathbb{R} - \{1, -1\} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{x^2 - 1}. \end{aligned}$$

In general, if f and g are any two functions, then we take the domain of the composite function $g \circ f$ to consist of all the elements in the domain of f such that $f(x)$ is in the domain of g. The codomain of $g \circ f$ is always the same as the codomain of g. So we have the following definition.

Definition

Let $f : A \longrightarrow B$ and $g : C \longrightarrow D$ be any two functions; then the **composite function** $g \circ f$ has:

- domain $\{x \in A : f(x) \in C\}$
- codomain D
- rule $(g \circ f)(x) = g(f(x))$.

This definition allows us to consider the composite of *any* two functions, though in some cases the domain may turn out to be the empty set $\varnothing$. However, some texts insist on $f(A) \subseteq C$ as a condition to ensure $g \circ f$ exists.

In the example above with

$$\begin{aligned} g \circ f : \mathbb{R} - \{1, -1\} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{x^2 - 1}, \end{aligned}$$

the domain of $g \circ f$ is just the set of values for which the rule of $g \circ f$ is defined. This is not always the case, as illustrated in the following worked exercise where the domain of f is not the whole of $\mathbb{R}$.

Worked Exercise A15

Determine the composite function $g \circ f$ for the following functions f and g:

$$\begin{aligned} f : [0, 2\pi) &\longrightarrow [-1, 1] \\ x &\longmapsto \sin x \end{aligned} \qquad \text{and} \qquad \begin{aligned} g : \mathbb{R} - \{-1\} &\longrightarrow \mathbb{R}^* \\ x &\longmapsto \frac{1}{x+1}. \end{aligned}$$

Solution

The composite function $g \circ f$ means f then g.

The rule of $g \circ f$ is

$$(g \circ f)(x) = g(f(x)) = g(\sin x) = \frac{1}{\sin x + 1}.$$

A number x is in the domain of $g \circ f$ if it is in the domain of f and $f(x)$ is in the domain of g.

The domain of $g \circ f$ is

$$\{x \in [0, 2\pi) : f(x) \in \mathbb{R} - \{-1\}\}.$$

If $x \in [0, 2\pi)$, then $f(x) \in \mathbb{R} - \{-1\}$ unless $f(x) = -1$.

Now $f(x) = -1$ means $\sin x = -1$, and the only value of x in $[0, 2\pi)$ such that $\sin x = -1$ is

$$x = \frac{3\pi}{2}.$$

The domain is complicated to write down so it helps to give it a name, say D.

So the domain of $g \circ f$ is

$$D = [0, 2\pi) - \{3\pi/2\}.$$

Thus $g \circ f$ is the function

$$\begin{aligned} g \circ f : D &\longrightarrow \mathbb{R}^* \\ x &\longmapsto \frac{1}{\sin x + 1}. \end{aligned}$$

Notice that, as claimed, in the worked exercise above the domain of $g \circ f$ is not the full set of values for which $g \circ f$ is defined. The full set of values for which $g \circ f$ is defined is

$$\{x \in \mathbb{R} : \sin x \neq -1\} = \mathbb{R} - \left\{\left(2n - \tfrac{1}{2}\right)\pi : n \in \mathbb{Z}\right\}.$$

Exercise A37

Determine the composite function $g \circ f$ for the following functions f and g:

$$\begin{aligned} f : [-1, 1] &\longrightarrow \mathbb{R} \\ x &\longmapsto 3x + 1 \end{aligned} \quad \text{and} \quad \begin{aligned} g : \mathbb{R} - \{-2\} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{3}{x+2}. \end{aligned}$$

Using function composition to show that a function is the inverse of another function

Suppose that $f : A \longrightarrow B$ is a one-to-one and onto function. Then f has an inverse function $f^{-1} : B \longrightarrow A$. We can therefore consider the effect that the composite function $f^{-1} \circ f : A \longrightarrow A$ has on an arbitrary element x in A. First, f maps x to an element $y = f(x)$ in B. Then f^{-1} 'undoes' the effect of f and maps y back to x, as illustrated in Figure 51. Overall, the effect of $f^{-1} \circ f$ is to leave x unchanged, or *fixed*: that is, $(f^{-1} \circ f)(x) = x$. Since x is an arbitrary element of A, it follows that $f^{-1} \circ f$ fixes all the elements of A. In other words, $f^{-1} \circ f = i_A$, the identity function on set A.

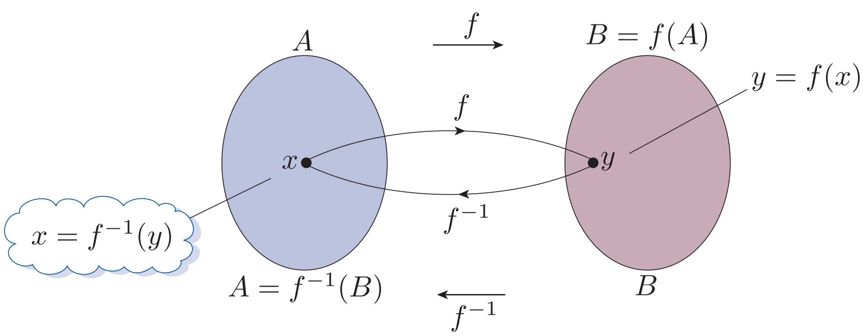


Figure 51 The composite function $f^{-1} \circ f$

A similar argument can be used to show that $f \circ f^{-1} = i_B$. So, if $f : A \longrightarrow B$ has an inverse function $f^{-1} : B \longrightarrow A$, then

$$f^{-1} \circ f = i_A \quad \text{and} \quad f \circ f^{-1} = i_B.$$

The *converse* of this statement is also true: that is, if a function $g : B \longrightarrow A$ satisfies

$$g \circ f = i_A \quad \text{and} \quad f \circ g = i_B,$$

then g is the inverse function of f. A proof of this is given after Exercise A39. It leads to the following strategy.

Strategy A2

To show that the function $g : B \longrightarrow A$ is the inverse function of the function $f : A \longrightarrow B$:

1. show that $g(f(x)) = x$ for each $x \in A$; that is, $g \circ f = i_A$
2. show that $f(g(y)) = y$ for each $y \in B$; that is, $f \circ g = i_B$.

In practice, we can sometimes use Strategy A2 as an alternative way of *finding* an inverse function. We make an inspired guess at the inverse function, and use Strategy A2 to check that our guess is correct.

Worked Exercise A16

Use Strategy A2 to find the inverse of the function

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \tfrac{1}{2}x. \end{aligned}$$

Solution

We guess that the inverse function is $g(x) = 2x$.

Let

$$\begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 2x. \end{aligned}$$

We use Strategy A2 to check that our guess is correct.

The domain of f is $\mathbb{R}$, and for each $x \in \mathbb{R}$ we have

$$g(f(x)) = g\left(\tfrac{1}{2}x\right) = 2 \times \tfrac{1}{2}x = x;$$

that is, $g \circ f = i_{\mathbb{R}}$.

The domain of g is also $\mathbb{R}$, and for each $y \in \mathbb{R}$ we have

$$f(g(y)) = f(2y) = \tfrac{1}{2} \times 2y = y;$$

that is, $f \circ g = i_{\mathbb{R}}$.

Since $g \circ f = i_{\mathbb{R}}$ and $f \circ g = i_{\mathbb{R}}$, it follows that g is the inverse function of f.

Exercise A38

Use Strategy A2 to show that g is the inverse of f, where

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 5x - 3 \end{aligned} \qquad \text{and} \qquad \begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{x+3}{5}. \end{aligned}$$

Exercise A39

Use Strategy A2 to find the inverse of the function

$$\begin{aligned} f &: \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x - 1, y + 3). \end{aligned}$$

To end this section, here is the promised proof that if the functions $f : A \longrightarrow B$ and $g : B \longrightarrow A$ satisfy

$$g \circ f = i_A \quad \text{and} \quad f \circ g = i_B,$$

then g is the inverse function of f. That is, we prove that if the two steps of Strategy A2 hold, then f has an inverse function, and the inverse function is equal to g.

Suppose, then, that the two steps of Strategy A2 hold. First we show that f is one-to-one.

Suppose that $f(x_1) = f(x_2)$; then

$$g(f(x_1)) = g(f(x_2)),$$

so, since $g(f(x)) = x$ for each $x \in A$ by the first step of Strategy A2, we have $x_1 = x_2$. Thus f is one-to-one and so it has an inverse function f^{-1}.

Now we find the image set of f.

We know that the image set of f is a subset of its codomain B, so $f(A) \subseteq B$. We now show that $f(A) \supseteq B$ by showing that every element y of B is the image under f of some element in A. Suppose that $y \in B$. Then, by the second step of Strategy A2,

$$f(g(y)) = y;$$

that is, y is the image under f of the element $g(y)$ and $g(y) \in A$, as required. Therefore $f(A) \supseteq B$.

Since $f(A) \subseteq B$ and $f(A) \supseteq B$, it follows that the image set of f is B (that is, f is onto), and so f^{-1} has domain B.

We now know that each of the functions f^{-1} and g has domain B and codomain A. To show that they are equal, it remains to show that $g(y) = f^{-1}(y)$ for each element y of B.

Let y be an arbitrary element of B. Then $y = f(x)$ for some element x of A. So

$$f^{-1}(y) = x,$$

and, by the first step of Strategy A2,

$$g(y) = g(f(x)) = x.$$

Hence f^{-1} and g are indeed equal functions.

4 Vectors

In this section you will revise vectors, in both the plane $\mathbb{R}^2$ and in three-dimensional space $\mathbb{R}^3$. Vectors are used throughout Book C *Linear algebra*.

4.1 What is a vector?

A mathematical or physical quantity that has a direction as well as a size is called a **vector**, or a **vector quantity**. An example of such a quantity is *velocity*: to state the velocity of a car you have to give its speed and also the direction in which it is moving. In contrast, some mathematical and physical quantities, such as temperature and volume, have only a size – they have no direction associated with them. We call such quantities **scalars**, or **scalar quantities**. When discussing vectors and scalars, we usually use the term **magnitude**, rather than size.

Definition

A **vector** is a quantity that is determined by its magnitude and direction. A **scalar** is a quantity that is determined by its magnitude.

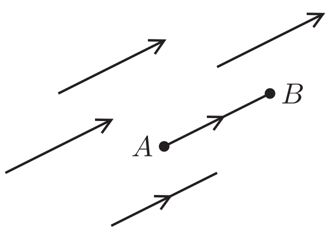


Figure 52 The same vector represented in different ways

We can represent a vector in $\mathbb{R}^2$ or in $\mathbb{R}^3$ geometrically by a line segment with an arrowhead, as illustrated in Figure 52. The length of the line segment is a measure of the magnitude of the vector, and the direction of the arrowhead indicates the direction. The starting point of the line segment does not matter; for example, all the line segments with arrowheads in Figure 52 represent the same vector. We can draw the arrowhead at the end of the line segment, or in the middle of it, as convenient. A vector represented by a line segment from A to B, with an arrowhead pointing from A to B, can be written as $\overrightarrow{AB}$.

Often we use single letters, such as $\mathbf{a}$, $\mathbf{b}$, $\mathbf{p}$, $\mathbf{q}$ or $\mathbf{v}$, to denote vectors. Vectors are usually distinguished in print by the use of a bold typeface, and in handwritten work by underlining the letters (for example, $\underline{v}$). These are important conventions as they clearly distinguish vector quantities from scalar quantities.

We denote the magnitude of a vector $\mathbf{v}$ by the notation $|\mathbf{v}|$.

There is one vector that does not fit conveniently into the definition above; namely, the *zero vector*. It represents any vector quantity that has magnitude zero and hence has no direction, such as the velocity of a stationary car.

Definition

The **zero vector** is the vector whose magnitude is zero, and whose direction is undefined. It is denoted by the symbol $\mathbf{0}$.

The next box defines what it means to say that two vectors are equal.

Definition

Two vectors **a** and **b** are **equal** if:

- they have the same magnitude; that is, $|\mathbf{a}| = |\mathbf{b}|$
- they are in the same direction.

We write $\mathbf{a} = \mathbf{b}$.

For example, in Figure 53, the vector $\mathbf{v}$ is equal to the vector $\mathbf{d}$, but is not equal to any of the other vectors, as they all differ from $\mathbf{v}$ in magnitude or direction.

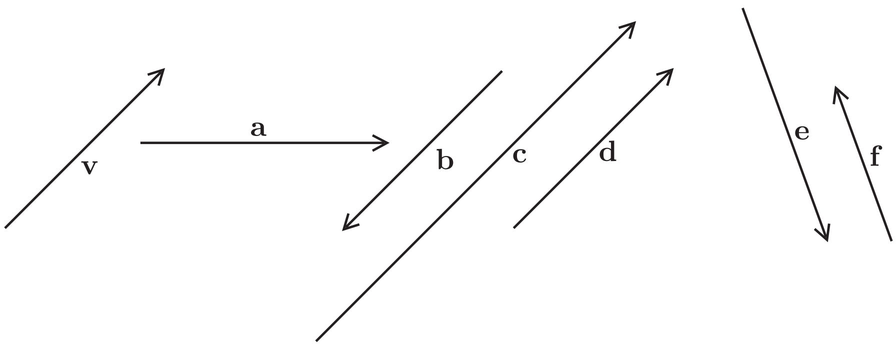


Figure 53 A selection of vectors in the plane

We now briefly revise some other definitions relating to vectors.

Definition

The **negative** of a vector $\mathbf{v}$ is the vector that has the same magnitude as $\mathbf{v}$, but the opposite direction. It is denoted by $-\mathbf{v}$.

For example, in Figure 53 we have $\mathbf{b} = -\mathbf{v}$. If we write $\mathbf{v}$ as $\overrightarrow{AB}$ for suitable points A and B, then $-\mathbf{v} = \overrightarrow{BA}$, as shown in Figure 54.

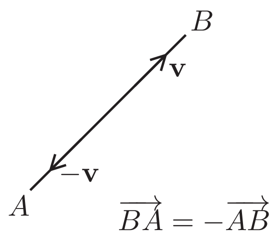


Figure 54 The vectors $\mathbf{v}$ and $-\mathbf{v}$

Scalar multiple of a vector

Let k be a scalar and $\mathbf{v}$ a vector. The **scalar multiple** $k\mathbf{v}$ of $\mathbf{v}$ is the vector:

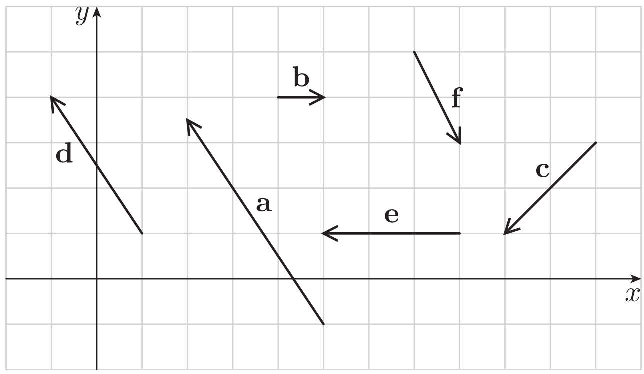
- whose magnitude is $|k|$ times the magnitude of $\mathbf{v}$; that is, $|k\mathbf{v}| = |k|\,|\mathbf{v}|$
- that has the same direction as $\mathbf{v}$ if $k > 0$, and the opposite direction if $k < 0$.

If $k = 0$, then $k\mathbf{v} = \mathbf{0}$.

For example, in Figure 53 we have $\mathbf{c} = 2\mathbf{v}$, since $\mathbf{c}$ has the same direction as $\mathbf{v}$ but twice the magnitude, and $\mathbf{e} = -\frac{3}{2}\mathbf{f}$, since $\mathbf{e}$ has the opposite direction to $\mathbf{f}$ and its magnitude is $\frac{3}{2}$ times that of $\mathbf{f}$.

Exercise A40

For each of the vectors shown below, decide whether it is a multiple of any of the other vectors; if it is, write down an equation of the form $\mathbf{v}_1 = k\mathbf{v}_2$ that specifies the relationship between them.



Exercise A41

For the vector $\mathbf{d}$ in Exercise A40, sketch $3\mathbf{d}$ and $-2\mathbf{d}$.

We can add two vectors using either of the two laws below. They give the same result, as illustrated in Figure 55.

Triangle Law for addition of vectors

The sum $\mathbf{p} + \mathbf{q}$ of two vectors $\mathbf{p}$ and $\mathbf{q}$ is obtained as follows.

1. Starting at any point, draw the vector $\mathbf{p}$.
2. Starting from the tip of the vector $\mathbf{p}$, draw the vector $\mathbf{q}$.

Then the sum $\mathbf{p} + \mathbf{q}$ is the vector from the tail of $\mathbf{p}$ to the tip of $\mathbf{q}$.

Parallelogram Law for addition of vectors

The sum $\mathbf{p} + \mathbf{q}$ of two vectors $\mathbf{p}$ and $\mathbf{q}$ is obtained as follows.

1. Starting at the same point, draw the vectors $\mathbf{p}$ and $\mathbf{q}$.
2. Complete the parallelogram of which these vectors are adjacent sides.

Then the sum $\mathbf{p} + \mathbf{q}$ is the vector from the point where the tails of $\mathbf{p}$ and $\mathbf{q}$ meet to the opposite corner of the parallelogram.

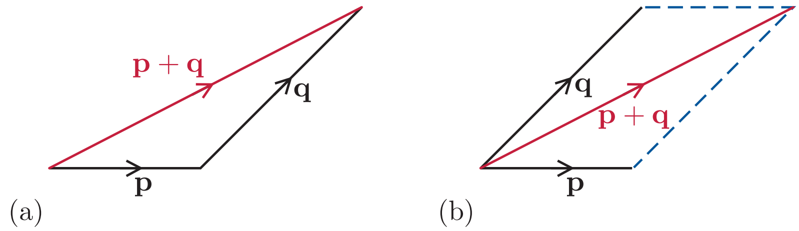


Figure 55 The sum $\mathbf{p}+\mathbf{q}$ obtained by (a) the Triangle Law (b) the Parallelogram Law

Addition and scalar multiplication of vectors obey the usual rules of algebra. The most important of these are listed in the box below.

Properties of vector algebra

Let $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$ be vectors, and let $a, b \in \mathbb{R}$. The following properties hold.

Commutativity $\quad \mathbf{p}+\mathbf{q}=\mathbf{q}+\mathbf{p}$

Associativity $\quad (\mathbf{p}+\mathbf{q})+\mathbf{r}=\mathbf{p}+(\mathbf{q}+\mathbf{r})$

Distributivity $\quad a(\mathbf{p}+\mathbf{q})=a\mathbf{p}+a\mathbf{q},$
$\quad (a+b)\mathbf{p}=a\mathbf{p}+b\mathbf{p}.$

Finally, we define subtraction of vectors in terms of addition and the negative of a vector, as follows, and as illustrated in Figure 56.

Definition

The **difference** $\mathbf{p}-\mathbf{q}$ of the vectors $\mathbf{p}$ and $\mathbf{q}$ is

$$\mathbf{p}-\mathbf{q}=\mathbf{p}+(-\mathbf{q}).$$

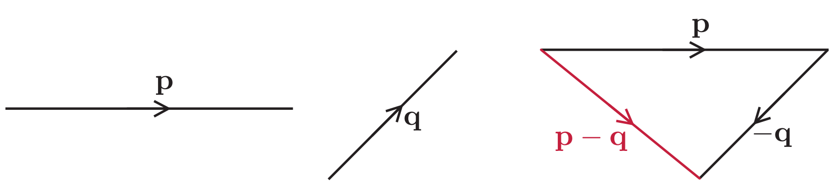


Figure 56 The difference $\mathbf{p}-\mathbf{q}$ of vectors $\mathbf{p}$ and $\mathbf{q}$

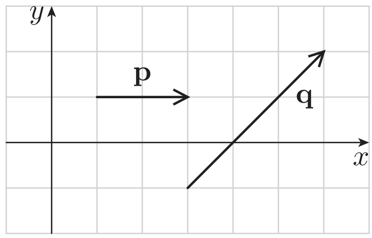
Since the vector $-\mathbf{q}$ has the same magnitude as $\mathbf{q}$ but the opposite direction, we can draw $\mathbf{p}-\mathbf{q}$ by using either of the two constructions that we use for adding vectors.

In general, $\mathbf{q}-\mathbf{p}$ does not equal $\mathbf{p}-\mathbf{q}$; in fact, as you would expect,

$$\mathbf{q}-\mathbf{p}=-(\mathbf{p}-\mathbf{q}).$$

Exercise A42

For the vectors $\mathbf{p}$ and $\mathbf{q}$ shown below, sketch $\mathbf{p}+\mathbf{q}$, $\mathbf{p}-\mathbf{q}$ and $2\mathbf{p}+\frac{1}{2}\mathbf{q}$.



4.2 Components and the arithmetic of vectors

We can sometimes simplify the manipulation of vectors by expressing them in *component form*. To do this, we start by defining the following *unit vectors*, shown in Figure 57. A **unit vector** is a vector of magnitude 1.

In $\mathbb{R}^2$, the vectors $\mathbf{i}$ and $\mathbf{j}$ are the unit vectors in the positive directions of the x- and y-axes, respectively.

In $\mathbb{R}^3$, the vectors $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ are the unit vectors in the positive directions of the x-, y- and z-axes, respectively.

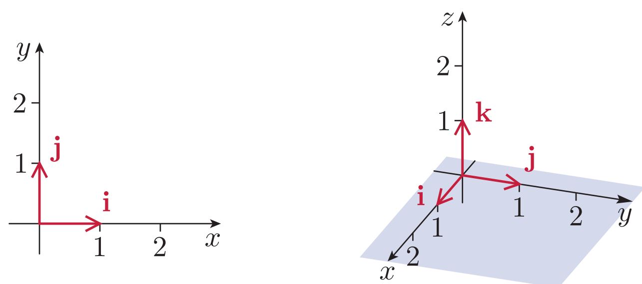


Figure 57 The unit vectors $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$

Any vector in $\mathbb{R}^2$ can be expressed as the sum of scalar multiples of $\mathbf{i}$ and $\mathbf{j}$, and similarly any vector in $\mathbb{R}^3$ can be expressed as the sum of scalar multiples of $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$. For example, the vector $\mathbf{v}$ in Figure 58(a) can be expressed as

$$\mathbf{v} = 3\mathbf{i} + 4\mathbf{j},$$

and the vector $\mathbf{w}$ in Figure 58(b) can be expressed as

$$\mathbf{w} = 2\mathbf{i} + 4\mathbf{j} + 3\mathbf{k}.$$

These expressions are the *component forms* of $\mathbf{v}$ and $\mathbf{w}$.

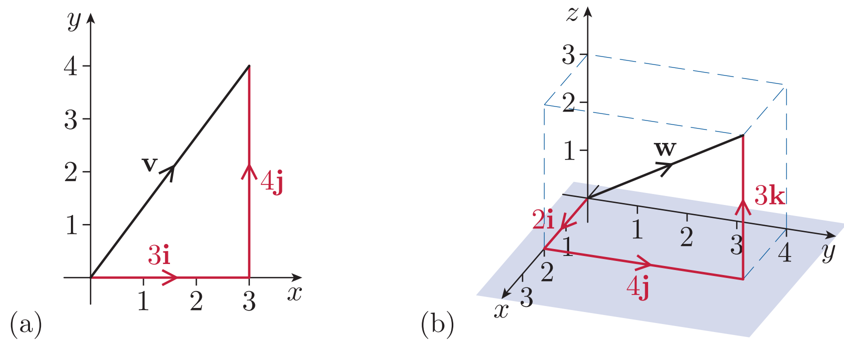


Figure 58 (a) A vector $\mathbf{v}$ in $\mathbb{R}^2$ (b) A vector $\mathbf{w}$ in $\mathbb{R}^3$

In general we have the following.

Definitions

Any vector $\mathbf{p}$ in $\mathbb{R}^2$ can be expressed in **component form** as

$$\mathbf{p} = a_1\mathbf{i} + a_2\mathbf{j}, \quad \text{for some real numbers } a_1, a_2;$$

we often write $\mathbf{p} = (a_1, a_2)$, for brevity. The numbers a_1 and a_2 are the **components** of $\mathbf{p}$ in the x- and y-directions, respectively.

Any vector $\mathbf{p}$ in $\mathbb{R}^3$ can be expressed in **component form** as

$$\mathbf{p} = a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, \quad \text{for some real numbers } a_1, a_2, a_3;$$

we often write $\mathbf{p} = (a_1, a_2, a_3)$, for brevity. The numbers a_1, a_2 and a_3 are the **components** of $\mathbf{p}$ in the x-, y- and z-directions, respectively.

So, for example, the component form of the vector $\mathbf{v}$ in Figure 58(a) is

$$3\mathbf{i} + 4\mathbf{j}, \quad \text{or, equivalently,} \quad (3, 4).$$

Similarly, the component form of the vector $\mathbf{w}$ in Figure 58(b) is

$$2\mathbf{i} + 4\mathbf{j} + 3\mathbf{k}, \quad \text{or, equivalently,} \quad (2, 4, 3).$$

In some texts, the ordered pairs and ordered triples that represent the component forms of vectors are written vertically, as

$$\begin{pmatrix} 3 \\ 4 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 \\ 4 \\ 3 \end{pmatrix},$$

for example, to distinguish them from points. Although we write them horizontally in this module, the meaning of an ordered pair or ordered triple should be clear from the context.

Exercise A43

Sketch the following vectors in $\mathbb{R}^2$ on a single diagram:

$$2\mathbf{i} - 3\mathbf{j}, \quad -3\mathbf{i} + 4\mathbf{j}, \quad -2\mathbf{i} - 2\mathbf{j}.$$

In the box below, the operations on vectors that were described geometrically in Subsection 4.1 are expressed in terms of components. The component forms of the vectors are expressed as ordered pairs and ordered triples in the box; there are analogous formulas for vectors expressed in terms of the unit vectors $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$. For example, the zero vector in $\mathbb{R}^2$ can be written as $\mathbf{0} = 0\mathbf{i} + 0\mathbf{j}$ rather than as $\mathbf{0} = (0, 0)$.

Vector arithmetic in component form

Equality Two vectors, both in $\mathbb{R}^2$ or both in $\mathbb{R}^3$, are equal if their corresponding components are equal.

Zero vector The zero vector is

$$\mathbf{0} = (0,0) \quad \text{in } \mathbb{R}^2,$$
$$\mathbf{0} = (0,0,0) \quad \text{in } \mathbb{R}^3.$$

Addition To add vectors in $\mathbb{R}^2$ or in $\mathbb{R}^3$, add their corresponding components:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$
$$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3).$$

Negatives To find the negative of a vector in $\mathbb{R}^2$ or in $\mathbb{R}^3$, take the negatives of its components:

$$-(a_1, a_2) = (-a_1, -a_2),$$
$$-(a_1, a_2, a_3) = (-a_1, -a_2, -a_3).$$

Subtraction To subtract vectors in $\mathbb{R}^2$ or in $\mathbb{R}^3$, subtract the corresponding components:

$$(a_1, a_2) - (b_1, b_2) = (a_1 - b_1, a_2 - b_2),$$
$$(a_1, a_2, a_3) - (b_1, b_2, b_3) = (a_1 - b_1, a_2 - b_2, a_3 - b_3).$$

Scalar multiplication To multiply a vector in $\mathbb{R}^2$ or in $\mathbb{R}^3$ by a real number k, multiply each component by k:

$$k(a_1, a_2) = (ka_1, ka_2),$$
$$k(a_1, a_2, a_3) = (ka_1, ka_2, ka_3).$$

Magnitude The magnitude of the vector (a_1, a_2) in $\mathbb{R}^2$ is

$$\sqrt{a_1^2 + a_2^2}.$$

The magnitude of the vector (a_1, a_2, a_3) in $\mathbb{R}^3$ is

$$\sqrt{a_1^2 + a_2^2 + a_3^2}.$$

The formulas for magnitude are derived from the distance formulas for $\mathbb{R}^2$ and $\mathbb{R}^3$ that you met in Section 1.

Here are some examples of vector arithmetic in component form, in $\mathbb{R}^2$: the sum of two vectors,

$$(1,-3)+(4,2)=(1+4,-3+2)=(5,-1),$$

the negative of a vector,

$$-(1,-3)=(-1,3),$$

and a scalar multiple of a vector,

$$2(2,-1)=(4,-2).$$

The magnitude of the vector $(1,-3)$ is given by

$$\sqrt{1^2+(-3)^2}=\sqrt{1+9}=\sqrt{10}.$$

Exercise A44

For each of the following pairs of vectors $\mathbf{p}$ and $\mathbf{q}$, write down $\mathbf{p}+\mathbf{q}$, $-\mathbf{q}$ and $\mathbf{p}-\mathbf{q}$.

(a) $\mathbf{p}=(3,-1)$ and $\mathbf{q}=(-1,-2)$.

(b) $\mathbf{p}=-\mathbf{i}-2\mathbf{j}$ and $\mathbf{q}=2\mathbf{i}-\mathbf{j}$.

(c) $\mathbf{p}=-\mathbf{i}+2\mathbf{k}$ and $\mathbf{q}=\mathbf{i}-2\mathbf{j}-\mathbf{k}$.

Exercise A45

For each of the following pairs of vectors $\mathbf{p}$ and $\mathbf{q}$, determine $2\mathbf{p}$, $3\mathbf{q}$ and $2\mathbf{p}-3\mathbf{q}$, and find the magnitude of $\mathbf{q}$.

(a) $\mathbf{p}=(3,-1)$ and $\mathbf{q}=(-1,-2)$.

(b) $\mathbf{p}=-\mathbf{i}+2\mathbf{k}$ and $\mathbf{q}=\mathbf{i}-2\mathbf{j}-\mathbf{k}$.

Unit vectors

As you saw earlier, a **unit vector** is a vector of magnitude 1. We denote the unit vector that is in the same direction as a particular vector $\mathbf{v}$ by $\widehat{\mathbf{v}}$ (read as 'v hat'), as illustrated in Figure 59.

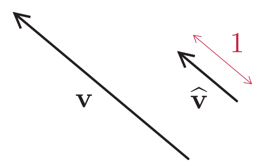


Figure 59 A vector $\mathbf{v}$ and its corresponding unit vector $\widehat{\mathbf{v}}$

To find $\widehat{\mathbf{v}}$, we multiply $\mathbf{v}$ by the reciprocal of its magnitude, as follows.

The unit vector in the same direction as a vector $\mathbf{v}$ is

$$\widehat{\mathbf{v}}=\frac{1}{|\mathbf{v}|}\mathbf{v}.$$

The exception to this notation for unit vectors is that we use the special symbols $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ for the unit vectors in the positive directions of the x-, y- and z-axes, as you saw earlier. This is common practice, though some texts use the alternative symbols $\widehat{\mathbf{x}}$, $\widehat{\mathbf{y}}$ and $\widehat{\mathbf{z}}$ for these vectors.

Worked Exercise A17

Find $\widehat{\mathbf{v}}$ for $\mathbf{v} = (3, 4)$.

Solution

For $\mathbf{v} = (3, 4)$ we have

$$|\mathbf{v}| = \sqrt{3^2 + 4^2} = \sqrt{25} = 5,$$

so

$$\widehat{\mathbf{v}} = \frac{1}{5}(3, 4) = \left(\frac{3}{5}, \frac{4}{5}\right).$$

Exercise A46

Find $\widehat{\mathbf{v}}$ for each of the following vectors $\mathbf{v}$.

(a) $(2, -3)$ (b) $5\mathbf{i} + 12\mathbf{j}$

Position vectors

There is a natural and useful way to associate every point in the plane or in three-dimensional space with a vector. We make the following definition.

Definition

Let P be any point in $\mathbb{R}^2$ or $\mathbb{R}^3$. The **position vector** of P is the vector whose starting point is the origin and whose finishing point is P, that is, the vector $\overrightarrow{OP}$, where O is the origin.

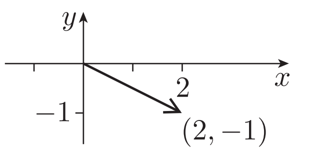


Figure 60 The position vector of the point $(2, -1)$

For example, the position vector of the point $P(2, -1)$ is the vector $\overrightarrow{OP} = 2\mathbf{i} - \mathbf{j}$ (often written as $(2, -1)$), as shown in Figure 60.

In general, any point (x, y) in $\mathbb{R}^2$ has position vector $x\mathbf{i} + y\mathbf{j}$ (often written as (x, y)), and similarly any point (x, y, z) in $\mathbb{R}^3$ has position vector $x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ (often written as (x, y, z)).

Exercise A47

Let $\mathbf{p}$ and $\mathbf{q}$ be the position vectors of the points $(5, 3)$ and $(1, 4)$, respectively.

(a) Determine the vectors $\mathbf{p} - \mathbf{q}$, $\mathbf{p} + \mathbf{q}$ and $\frac{1}{2}\mathbf{p} + \frac{1}{2}\mathbf{q}$.

(b) Sketch $\mathbf{p}$, $\mathbf{q}$ and each of the vectors that you found in part (a), starting each vector at the origin.

The following simple result about position vectors is often useful.

Let A and B be points (in $\mathbb{R}^2$ or $\mathbb{R}^3$), with position vectors $\mathbf{a}$ and $\mathbf{b}$, respectively. Then

$$\overrightarrow{AB} = \mathbf{b} - \mathbf{a}.$$

To see this, let O be the origin, as shown in Figure 61. Then

$$\begin{aligned}\overrightarrow{AB} &= \overrightarrow{AO} + \overrightarrow{OB} \quad \text{(by the Triangle Law for vector addition)}\\ &= -\overrightarrow{OA} + \overrightarrow{OB}\\ &= -\mathbf{a} + \mathbf{b}\\ &= \mathbf{b} - \mathbf{a},\end{aligned}$$

as claimed.

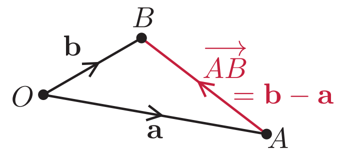


Figure 61 Points A and B and their position vectors

The sets $\mathbb{R}^2$ and $\mathbb{R}^3$

Finally, we clarify some issues about the sets $\mathbb{R}^2$ and $\mathbb{R}^3$. You have seen that we use the notation $\mathbb{R}^2$ to denote the plane, and the notation $\mathbb{R}^3$ to denote three-dimensional space. Strictly, the meaning of these notations is as follows:

$$\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\},$$
$$\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}.$$

That is, $\mathbb{R}^2$ is the set of all ordered pairs of real numbers, and $\mathbb{R}^3$ is the set of all ordered triples of real numbers. We interpret these sets as the plane and as three-dimensional space, respectively, by interpreting their elements as the coordinates of points with respect to particular coordinate systems, in the way that you have seen.

However, it is often useful to instead interpret the elements of $\mathbb{R}^2$ and $\mathbb{R}^3$ as *vectors*. For example, we can interpret the element $(2, -1)$ of $\mathbb{R}^2$ not as the point with coordinates $(2, -1)$, but instead as the vector with component form $(2, -1)$.

We can use whichever interpretation of $\mathbb{R}^2$ and $\mathbb{R}^3$ is more useful in a particular context. A link between the two interpretations is provided by position vectors, because the vector with component form (x, y) is the position vector of the point with coordinates (x, y), and similarly the vector with component form (x, y, z) is the position vector of the point with coordinates (x, y, z).

This link also makes it straightforward to represent a particular point not by coordinates, but by a vector: we use its position vector. It might seem that this amounts to much the same thing, but the advantage of representing points by vectors is that it enables us to use the properties of vectors to work with points. This leads to some very convenient ways of working with points, as you will see in the next subsection and again in Subsection 4.5. In Book C you will see how generalising all these ideas leads to some interesting and very useful mathematics.

4.3 Vector form of the equation of a line

In Subsection 1.1, we found that every line in the plane has an equation of the form

$$ax + by = c,$$

where a, b and c are real numbers, with a and b not both zero. In this subsection we find an equivalent general form for the equation of a line in terms of vectors. Unlike the equation above, this vector form applies to lines in $\mathbb{R}^3$ as well as in $\mathbb{R}^2$, as you will see later in this subsection.

Let P and Q be points with position vectors $\mathbf{p}$ and $\mathbf{q}$, respectively, and let l be the line that passes through P and Q, as illustrated in Figure 62. We now find an expression for the position vector $\mathbf{r}$ of an arbitrary point R on l in terms of the position vectors $\mathbf{p}$ and $\mathbf{q}$.

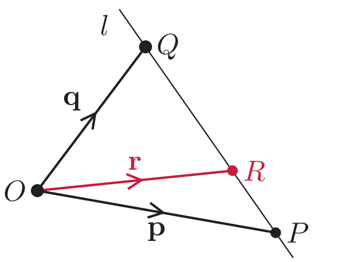


Figure 62 A point R on the line l

Since the vector $\overrightarrow{PR}$ is parallel to the vector $\overrightarrow{PQ}$, it must be a multiple of $\overrightarrow{PQ}$, that is,

$$\overrightarrow{PR} = \lambda \overrightarrow{PQ},$$

for some real number λ. Now, by the result about position vectors given at the end of the last subsection, we have

$$\overrightarrow{PR} = \mathbf{r} - \mathbf{p} \quad \text{and} \quad \overrightarrow{PQ} = \mathbf{q} - \mathbf{p}.$$

So

$$\mathbf{r} - \mathbf{p} = \lambda(\mathbf{q} - \mathbf{p}).$$

We can rearrange this equation as

$$\mathbf{r} = \mathbf{p} + \lambda(\mathbf{q} - \mathbf{p}),$$

that is,

$$\mathbf{r} = (1 - \lambda)\mathbf{p} + \lambda\mathbf{q}. \tag{3}$$

This is a general formula for the position vector of a point on the line through P and Q, in the following sense: each point on l corresponds to a particular value of λ, and vice versa. As shown in Figure 63, we have the following.

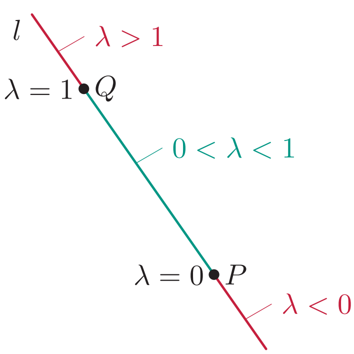


Figure 63 The position of R determined by λ

- If $\lambda = 0$, then $\mathbf{r} = 1\mathbf{p} + 0\mathbf{q} = \mathbf{p}$.
- If $\lambda = 1$, then $\mathbf{r} = 0\mathbf{p} + 1\mathbf{q} = \mathbf{q}$.
- If $\lambda > 1$, then R lies on l beyond Q.
- If $0 < \lambda < 1$, then R lies on l between P and Q.
- If $\lambda < 0$, then R lies on l beyond P.

So we can regard equation (3) as the *vector form of the equation of the line l*.

Vector form of the equation of a line

The equation of the line through the points with position vectors $\mathbf{p}$ and $\mathbf{q}$ is

$$\mathbf{r} = (1-\lambda)\mathbf{p} + \lambda\mathbf{q}, \quad \text{where } \lambda \in \mathbb{R}.$$

Note in particular that when $\lambda = \frac{1}{2}$ in the equation above, we have $\mathbf{r} = \frac{1}{2}\mathbf{p} + \frac{1}{2}\mathbf{q} = \frac{1}{2}(\mathbf{p}+\mathbf{q})$, which is the position vector of the *midpoint* of the line segment PQ.

Worked Exercise A18

(a) Let P and Q be the points with position vectors $\mathbf{p} = (1,3)$ and $\mathbf{q} = (-1,-2)$, respectively. Find the vector form of the equation of the line l through P and Q.

(b) Determine whether the point $(3,8)$ lies on l.

Solution

(a) The vector form of the equation of the line l is

$$\mathbf{r} = (1-\lambda)(1,3) + \lambda(-1,-2),$$

that is,

$$\mathbf{r} = (1-2\lambda, 3-5\lambda),$$

where $\lambda \in \mathbb{R}$.

(b) The point $(3,8)$ lies on the line if there is some real number λ such that

$$(3,8) = (1-2\lambda, 3-5\lambda).$$

Equating the corresponding components gives

$$3 = 1-2\lambda \quad \text{and} \quad 8 = 3-5\lambda.$$

The first equation gives $\lambda = -1$, and this value of λ also satisfies the other equation. Hence the point $(3,8)$ does lie on the line l.

Exercise A48

Let P and Q be the points with position vectors $\mathbf{p} = (3,1)$ and $\mathbf{q} = (2,3)$, respectively. Let l be the line through P and Q.

(a) Find the vector form of the equation of the line l.

(b) Determine the three points on l whose position vectors are given by the equation you found in part (a) when λ takes the values $\frac{2}{3}$, $\frac{3}{2}$ and $-\frac{1}{2}$, respectively.

(c) On a single diagram, sketch P, Q, the line l through P and Q, and the three points that you found in part (b).

Exercise A49

Let P, Q and l be as in Exercise A48.

(a) Determine the value of λ corresponding to the point $(4, -1)$ in the vector form of the equation of l.

(b) Use the vector form of the equation of l to prove that the point $\left(\frac{1}{2}, \frac{1}{2}\right)$ does not lie on l.

In the vector form of the equation of a line, there is no assumption that $\mathbf{p}$ and $\mathbf{q}$ are position vectors of points in $\mathbb{R}^2$: they may equally well be position vectors in $\mathbb{R}^3$.

Worked Exercise A19

(a) Let P and Q be the points with position vectors $\mathbf{p} = (1, 2, 3)$ and $\mathbf{q} = (3, -2, 1)$, respectively. Find the vector form of the equation of the line l through P and Q.

(b) Determine whether the point $(4, -4, 0)$ lies on the line l.

Solution

(a) The vector form of the equation of l is

$$\begin{aligned}\mathbf{r} &= (1-\lambda)(1, 2, 3) + \lambda(3, -2, 1)\\ &= (1 + 2\lambda,\ 2 - 4\lambda,\ 3 - 2\lambda), \quad \text{where } \lambda \in \mathbb{R}.\end{aligned}$$

(b) The point $(4, -4, 0)$ lies on the line l if there is a real number λ such that

$$\begin{aligned}1 + 2\lambda &= 4,\\ 2 - 4\lambda &= -4,\\ 3 - 2\lambda &= 0.\end{aligned}$$

The first equation gives $\lambda = \frac{3}{2}$, and this value of λ also satisfies the other two equations. Hence the point $(4, -4, 0)$ lies on the line l.

Exercise A50

(a) Let P and Q be the points with position vectors $\mathbf{p} = (2, 1, 0)$ and $\mathbf{q} = (1, 0, -1)$, respectively. Find the vector form of the equation of the line l through P and Q.

(b) Determine the points on l whose position vectors are given by the equation you found in part (a) when λ takes the values $\frac{1}{2}$ and -1.

4.4 Scalar product

In this subsection you will meet a way of combining two vectors, known as the *scalar product* or *dot product*, which is useful in linear algebra, as you will see in Book C.

The definition of the scalar product is given below. It applies to vectors in both $\mathbb{R}^2$ and $\mathbb{R}^3$.

Definition

If $\mathbf{u}$ and $\mathbf{v}$ are non-zero vectors in $\mathbb{R}^2$ or $\mathbb{R}^3$, then the **scalar product** (or **dot product**) of $\mathbf{u}$ and $\mathbf{v}$ is

$$\mathbf{u}\cdot\mathbf{v} = |\mathbf{u}||\mathbf{v}|\cos\theta,$$

where θ is the angle between $\mathbf{u}$ and $\mathbf{v}$.

If one or both of $\mathbf{u}$ and $\mathbf{v}$ is the zero vector, then $\mathbf{u}\cdot\mathbf{v} = 0$.

The scalar product of two vectors is a scalar, hence the name.

Note that the angle between two vectors is defined to be the angle θ in the range $0 \leq \theta \leq \pi$ between their directions when the vectors are placed to have the same starting point (not necessarily the origin), as illustrated in Figure 64 for vectors in $\mathbb{R}^2$ and $\mathbb{R}^3$.

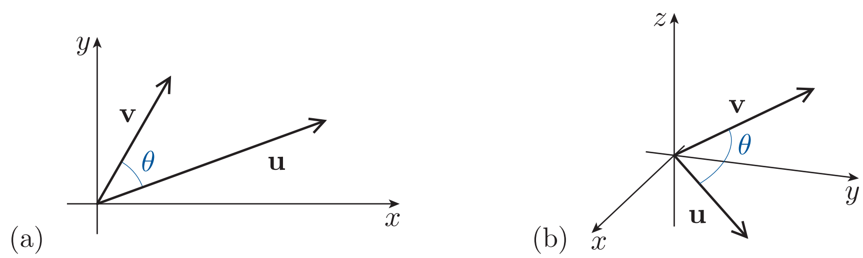


Figure 64 The angle θ between two vectors $\mathbf{u}$ and $\mathbf{v}$ in (a) $\mathbb{R}^2$ and (b) $\mathbb{R}^3$

Let us use the definition of the scalar product to calculate the scalar product $\mathbf{u}\cdot\mathbf{v}$ of the vectors $\mathbf{u} = (2, 0)$ and $\mathbf{v} = (3, 3)$ in $\mathbb{R}^2$, which are shown in Figure 65. We have

$$|\mathbf{u}| = 2$$

and

$$|\mathbf{v}| = \sqrt{3^2 + 3^2} = \sqrt{2 \times 3^2} = 3\sqrt{2}.$$

The angle θ between the vectors $\mathbf{u}$ and $\mathbf{v}$ is $\pi/4$. Hence

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} &= |\mathbf{u}||\mathbf{v}|\cos\theta \\ &= 2 \times 3\sqrt{2} \times \cos\frac{\pi}{4} \\ &= 6\sqrt{2} \times \frac{1}{\sqrt{2}} \\ &= 6.\end{aligned}$$

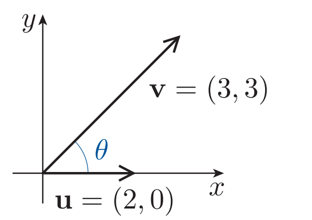


Figure 65 The vectors $\mathbf{u} = (2, 0)$ and $\mathbf{v} = (3, 3)$

There is an easier way to calculate the scalar product of two vectors, which does not depend on knowing the angle between them, but just involves their components. You will meet this method shortly, but first we will use the definition of the scalar product to derive some of its properties.

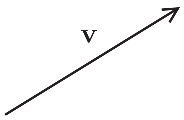


Figure 66 A vector $\mathbf{v}$

To start with, consider any vector $\mathbf{v}$ in $\mathbb{R}^2$ or $\mathbb{R}^3$, as illustrated in Figure 66. Let us find the scalar product of $\mathbf{v}$ with itself. The angle between $\mathbf{v}$ and itself is 0, so we have

$$\mathbf{v} \cdot \mathbf{v} = |\mathbf{v}||\mathbf{v}| \cos 0 = |\mathbf{v}|^2 \times 1 = |\mathbf{v}|^2.$$

This gives the following property.

Magnitude of a vector in terms of scalar product

For any vector $\mathbf{v}$ in $\mathbb{R}^2$ or $\mathbb{R}^3$,

$$|\mathbf{v}| = \sqrt{\mathbf{v} \cdot \mathbf{v}}.$$

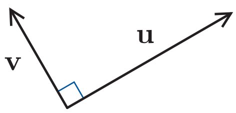


Figure 67 Perpendicular vectors $\mathbf{u}$ and $\mathbf{v}$

Now consider any two vectors $\mathbf{u}$ and $\mathbf{v}$ in $\mathbb{R}^2$ or $\mathbb{R}^3$ that are at right angles to each other, as illustrated in Figure 67. Their scalar product is

$$\mathbf{u} \cdot \mathbf{v} = |\mathbf{u}||\mathbf{v}| \cos \frac{\pi}{2} = |\mathbf{u}||\mathbf{v}| \times 0 = 0.$$

So the scalar product of any two perpendicular vectors is 0.

A *converse* of this result also holds. Suppose that $\mathbf{u}$ and $\mathbf{v}$ are vectors in $\mathbb{R}^2$ or $\mathbb{R}^3$ whose scalar product is 0. Then, by the definition of the scalar product,

$$|\mathbf{u}||\mathbf{v}| \cos \theta = 0,$$

where θ is the angle between $\mathbf{u}$ and $\mathbf{v}$. It follows that

$$|\mathbf{u}| = 0 \quad \text{or} \quad |\mathbf{v}| = 0 \quad \text{or} \quad \cos \theta = 0,$$

and hence

$$\mathbf{u} = \mathbf{0} \quad \text{or} \quad \mathbf{v} = \mathbf{0} \quad \text{or} \quad \theta = \frac{\pi}{2}.$$

So we have the following property.

Scalar product and perpendicularity

Let $\mathbf{u}$ and $\mathbf{v}$ be vectors.

- If $\mathbf{u}$ and $\mathbf{v}$ are perpendicular, then $\mathbf{u} \cdot \mathbf{v} = 0$.
- If $\mathbf{u} \cdot \mathbf{v} = 0$, then $\mathbf{u} = \mathbf{0}$, or $\mathbf{v} = \mathbf{0}$, or $\mathbf{u}$ and $\mathbf{v}$ are perpendicular.

Finally, the scalar product has the following algebraic properties.

Algebraic properties of scalar product

Let $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ be vectors in $\mathbb{R}^2$ or $\mathbb{R}^3$, and let $\alpha \in \mathbb{R}$. The following properties hold.

Commutativity $\quad \mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$

Multiples $\quad (\alpha\mathbf{u}) \cdot \mathbf{v} = \mathbf{u} \cdot (\alpha\mathbf{v}) = \alpha(\mathbf{u} \cdot \mathbf{v})$

Distributivity $\quad \mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w},$
$\quad (\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w}.$

Note that the distributive properties in the box also hold if the plus signs are replaced by minus signs. This follows by combining the distributive properties with the multiples property for $\alpha = -1$.

The properties of the scalar product in the box can be proved by using the definition of the scalar product.

The commutative property follows immediately from the definition.

To see why the multiples property holds, let $\mathbf{u}$ and $\mathbf{v}$ be two vectors in $\mathbb{R}^2$ or $\mathbb{R}^3$, and first suppose that α is a *positive* constant. If the angle between $\mathbf{u}$ and $\mathbf{v}$ is θ, then the angle between $\alpha\mathbf{u}$ and $\mathbf{v}$ is also θ, as illustrated in Figure 68, so

$$\begin{aligned}
(\alpha\mathbf{u}) \cdot \mathbf{v} &= |\alpha\mathbf{u}||\mathbf{v}| \cos\theta \\
&= |\alpha||\mathbf{u}||\mathbf{v}| \cos\theta \\
&= \alpha|\mathbf{u}||\mathbf{v}| \cos\theta \qquad \text{(since } \alpha \text{ is positive)} \\
&= \alpha(\mathbf{u} \cdot \mathbf{v}),
\end{aligned}$$

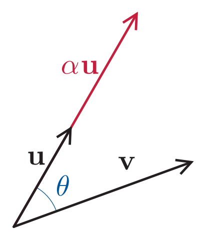


Figure 68 Vectors $\mathbf{u}$ and $\mathbf{v}$, and a scalar multiple $\alpha\mathbf{u}$ of $\mathbf{u}$, where α is positive

and, similarly,

$$\begin{aligned}
\mathbf{u} \cdot (\alpha\mathbf{v}) &= |\mathbf{u}||\alpha\mathbf{v}| \cos\theta \\
&= |\mathbf{u}||\alpha||\mathbf{v}| \cos\theta \\
&= \alpha|\mathbf{u}||\mathbf{v}| \cos\theta \\
&= \alpha(\mathbf{u} \cdot \mathbf{v}).
\end{aligned}$$

The multiples property can be proved in the case where α is negative in a similar way. In this case the angle between $\alpha\mathbf{u}$ and $\mathbf{v}$, and also the angle between $\mathbf{u}$ and $\alpha\mathbf{v}$, is $\pi - \theta$, but $\cos(\pi - \theta) = -\cos\theta$ by the properties of the cosine function (see the module Handbook).

The proof of the distributive properties is more complicated, and the details are omitted here.

Using the properties of the scalar product given above, we can prove the following simple formulas for calculating the scalar product.

Scalar product of vectors in component form

In $\mathbb{R}^2$, let $\mathbf{u} = (x_1, y_1)$ and $\mathbf{v} = (x_2, y_2)$. Then

$$\mathbf{u} \cdot \mathbf{v} = x_1x_2 + y_1y_2.$$

In $\mathbb{R}^3$, let $\mathbf{u} = (x_1, y_1, z_1)$ and $\mathbf{v} = (x_2, y_2, z_2)$. Then

$$\mathbf{u} \cdot \mathbf{v} = x_1x_2 + y_1y_2 + z_1z_2.$$

Here is a proof of the formula above for vectors in $\mathbb{R}^2$. The proof for vectors in $\mathbb{R}^3$ is similar, but longer.

Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbb{R}^2$. We write them in component form as

$$\mathbf{u} = x_1\mathbf{i} + y_1\mathbf{j} \quad \text{and} \quad \mathbf{v} = x_2\mathbf{i} + y_2\mathbf{j},$$

as shown in Figure 69 below.

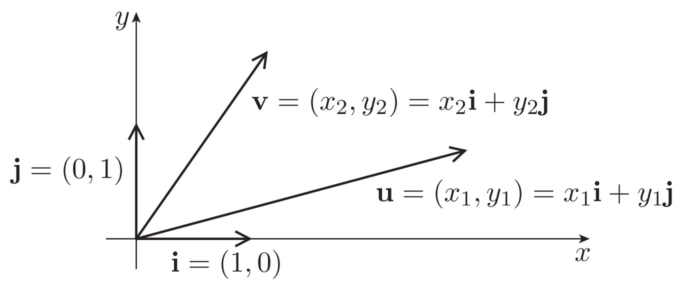


Figure 69 The vectors $\mathbf{u}$ and $\mathbf{v}$ in component form

This gives

$$\begin{aligned}
\mathbf{u} \cdot \mathbf{v} &= (x_1\mathbf{i} + y_1\mathbf{j}) \cdot (x_2\mathbf{i} + y_2\mathbf{j}) \\
&= (x_1\mathbf{i} + y_1\mathbf{j}) \cdot x_2\mathbf{i} + (x_1\mathbf{i} + y_1\mathbf{j}) \cdot y_2\mathbf{j} \quad \text{(by distributivity)} \\
&= x_1\mathbf{i} \cdot x_2\mathbf{i} + y_1\mathbf{j} \cdot x_2\mathbf{i} + x_1\mathbf{i} \cdot y_2\mathbf{j} + y_1\mathbf{j} \cdot y_2\mathbf{j} \\
&\qquad \text{(by distributivity)} \\
&= x_1x_2\mathbf{i} \cdot \mathbf{i} + y_1x_2\mathbf{j} \cdot \mathbf{i} + x_1y_2\mathbf{i} \cdot \mathbf{j} + y_1y_2\mathbf{j} \cdot \mathbf{j} \\
&\qquad \text{(by the multiples property).}
\end{aligned}$$

Now $\mathbf{i}$ and $\mathbf{j}$ have magnitude 1, so by the formula for the magnitude of a vector in terms of scalar product, given earlier,

$$\mathbf{i} \cdot \mathbf{i} = 1^2 = 1 \quad \text{and} \quad \mathbf{j} \cdot \mathbf{j} = 1^2 = 1.$$

Also, $\mathbf{i}$ and $\mathbf{j}$ are perpendicular, so

$$\mathbf{i} \cdot \mathbf{j} = \mathbf{j} \cdot \mathbf{i} = 0.$$

Hence

$$\begin{aligned}
\mathbf{u} \cdot \mathbf{v} &= x_1x_2 \times 1 + y_1x_2 \times 0 + x_1y_2 \times 0 + y_1y_2 \times 1 \\
&= x_1x_2 + y_1y_2,
\end{aligned}$$

as claimed.

Worked Exercise A20

Calculate the following scalar products.

(a) $(3,3)\cdot(2,0)$ (b) $(2\mathbf{i}+3\mathbf{j})\cdot(2\mathbf{i}-\mathbf{j})$ (c) $(\sqrt{2},-4)\cdot(2\sqrt{2},1)$

(d) $(1,-1,1)\cdot(1,-1,1)$

Solution

(a) $$\begin{aligned}(3,3)\cdot(2,0) &= 3\times 2+3\times 0\\ &= 6+0=6\end{aligned}$$

(b) $$\begin{aligned}(2\mathbf{i}+3\mathbf{j})\cdot(2\mathbf{i}-\mathbf{j}) &= 2\times 2+3\times(-1)\\ &= 4-3=1\end{aligned}$$

(c) $$\begin{aligned}(\sqrt{2},-4)\cdot(2\sqrt{2},1) &= \sqrt{2}\times 2\sqrt{2}-4\times 1\\ &= 4-4=0\end{aligned}$$

(d) $$\begin{aligned}(1,-1,1)\cdot(1,-1,1) &= 1\times 1+(-1)\times(-1)+1\times 1\\ &= 1+1+1=3\end{aligned}$$

Worked Exercise A20(a) is the particular scalar product that was calculated using the original definition near the start of this subsection.

Notice that the result of Worked Exercise A20(c) shows that the vectors $(\sqrt{2},-4)$ and $(2\sqrt{2},1)$ are perpendicular, something that is not immediately obvious when we look at their component forms.

Exercise A51

Calculate the following scalar products.

(a) $(2,3)\cdot\left(\frac{5}{2},-4\right)$ (b) $(1,4)\cdot\left(2,-\frac{1}{2}\right)$ (c) $(-2\mathbf{i}+\mathbf{j})\cdot(3\mathbf{i}-2\mathbf{j})$

(d) $(1,-1,-2)\cdot(3,-2,-5)$

One useful application of the scalar product is that it provides a method for finding the angle between two vectors, as illustrated in Figure 70. The formula below is obtained by rearranging the original definition of the scalar product.

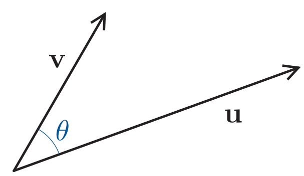


Figure 70 Two vectors $\mathbf{u}$ and $\mathbf{v}$, and the angle θ between them

Angle between two vectors

The angle θ between two vectors $\mathbf{u}$ and $\mathbf{v}$ is given by

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|}.$$

In the next worked exercise this formula is used to find the angle between two vectors in $\mathbb{R}^2$.

Worked Exercise A21

Find the angle θ between the vectors $\mathbf{u} = (4, -2)$ and $\mathbf{v} = (9, 3)$, in radians. (These vectors are shown in Figure 71.)

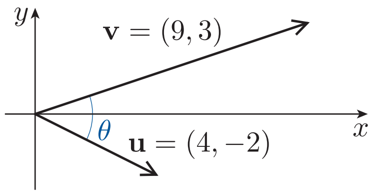


Figure 71 The vectors $\mathbf{u} = (4, -2)$ and $\mathbf{v} = (9, 3)$

Solution

We have

$$\mathbf{u} \cdot \mathbf{v} = 4 \times 9 + (-2) \times 3 = 36 - 6 = 30,$$

$$|\mathbf{u}| = \sqrt{4^2 + (-2)^2} = \sqrt{20} = 2\sqrt{5},$$

$$|\mathbf{v}| = \sqrt{9^2 + 3^2} = \sqrt{90} = 3\sqrt{10}.$$

So

$$\cos\theta = \frac{\mathbf{u} \cdot \mathbf{v}}{|\mathbf{u}||\mathbf{v}|} = \frac{30}{2\sqrt{5} \times 3\sqrt{10}} = \frac{30}{30\sqrt{2}} = \frac{1}{\sqrt{2}}.$$

For the angle between the two vectors, we need to choose the value of θ that satisfies this equation and lies in the range $0 \leq \theta \leq \pi$.

Hence

$$\theta = \cos^{-1}\left(\frac{1}{\sqrt{2}}\right) = \frac{\pi}{4}.$$

Exercise A52

Find the angle between the vectors in each of the following pairs of vectors, in radians. Give your answer to two decimal places unless it is an obvious multiple of π.

(a) $(1, 4)$, $(5, 2)$ (b) $(-2, 2)$, $(1, -1)$ (c) $9\mathbf{i} - 2\mathbf{j}$, $\mathbf{i} + 2\mathbf{j}$

The formula for the angle between two vectors works equally well in $\mathbb{R}^3$, as is shown in the next worked exercise.

Worked Exercise A22

Find the angle θ between the vectors $\mathbf{u} = (3, 1, -1)$ and $\mathbf{v} = (1, 2, 3)$, in radians to two decimal places. (These vectors are shown in Figure 72.)

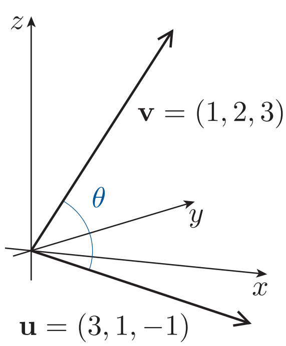


Figure 72 The vectors $\mathbf{u} = (3, 1, -1)$ and $\mathbf{v} = (1, 2, 3)$

Solution

We have

$$\mathbf{u}\cdot\mathbf{v} = 3\times 1 + 1\times 2 + (-1)\times 3 = 2,$$

$$|\mathbf{u}| = \sqrt{3^2+1^2+(-1)^2} = \sqrt{11},$$

$$|\mathbf{v}| = \sqrt{1^2+2^2+3^2} = \sqrt{14}.$$

So

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|} = \frac{2}{\sqrt{11}\sqrt{14}} = \frac{2}{\sqrt{154}}.$$

Hence

$$\theta = \cos^{-1}\left(\frac{2}{\sqrt{154}}\right) = 1.41 \text{ radians (to 2 d.p.)}.$$

Exercise A53

Find the angle between the following pairs of vectors, in radians to two decimal places.

(a) $(3,4,5)$, $(1,0,-1)$

(b) $2\mathbf{j}-3\mathbf{k}$, $-\mathbf{i}-\mathbf{j}-2\mathbf{k}$

4.5 Equation of a plane in $\mathbb{R}^3$

In Subsection 1.1 you saw that the general form of the equation of a line in $\mathbb{R}^2$ is $ax+by=c$, where $a,b,c\in\mathbb{R}$, and a and b are not both zero. We can use the scalar product to derive a similar general form for the equation of a plane in $\mathbb{R}^3$, as you will see in this subsection. In doing this, we will also derive a general form for the equation of a plane in $\mathbb{R}^3$ in terms of vectors.

First, let us look at some planes in $\mathbb{R}^3$ whose equations are easy to find. The 'simplest' planes in $\mathbb{R}^3$ are the three planes that contain a pair of axes. The (x,y)**-plane** is the plane that contains the x- and y-axes, as illustrated in Figure 73. The (x,z)**-plane** and the (y,z)**-plane** are defined similarly. The points that lie in the (x,y)-plane are the points (x,y,z) in $\mathbb{R}^3$ for which $z=0$, so the equation of the (x,y)-plane is

$$z=0.$$

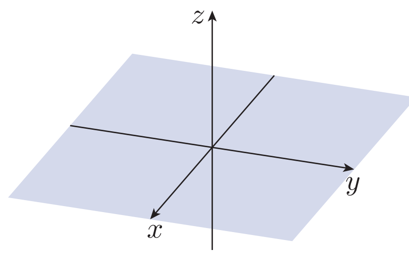


Figure 73 The (x,y)-plane

Exercise A54

Write down the equations of the (y, z)-plane and the (x, z)-plane.

Exercise A55

Sketch the planes whose equations are as follows.

(a) $z = 2$ (b) $y = -1$

Before we derive the general equation of a plane in $\mathbb{R}^3$, we need the following concept.

Definition

A vector that is perpendicular to all the vectors in a particular plane is called a **normal vector** (or simply a **normal**) to the plane. Its direction is said to be **normal** to the plane.

Figure 74(a) shows some normal vectors to a plane. If $\mathbf{n}$ is a normal vector to a particular plane, then so is $k\mathbf{n}$, for any non-zero real number k. If $k > 0$, then $k\mathbf{n}$ is in the same direction as $\mathbf{n}$, whereas if $k < 0$, then $k\mathbf{n}$ is in the opposite direction to $\mathbf{n}$, as illustrated in Figure 74(b).

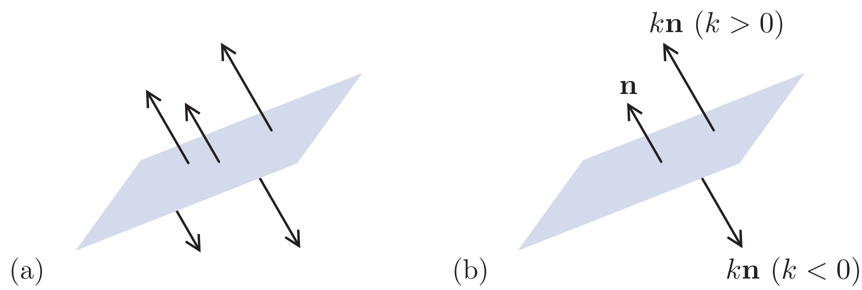


Figure 74 Some normal vectors to a plane

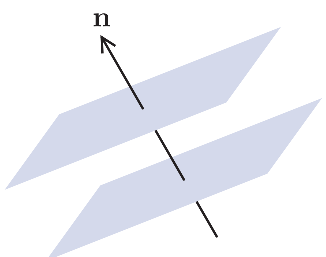


Figure 75 Parallel planes

Any vector $\mathbf{n}$ in $\mathbb{R}^3$ is a normal vector to infinitely many planes, all parallel to each other, as illustrated in Figure 75.

We can specify any particular plane in $\mathbb{R}^3$ by specifying a normal vector to the plane, together with a point that lies in the plane. For example, there is exactly one plane that contains the point $P(2, 3, 4)$ and has $\mathbf{n} = (1, 2, -1)$ as a normal.

Here is how we can find an equation for this particular plane. A condition for an arbitrary point $X(x, y, z)$ in $\mathbb{R}^3$ to lie in the plane is that the vector $\overrightarrow{PX}$ must be perpendicular to the normal vector $\mathbf{n}$, as illustrated in Figure 76. In other words, we must have

$$\overrightarrow{PX} \cdot \mathbf{n} = 0.$$

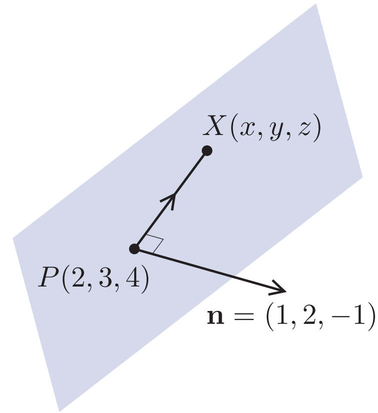


Figure 76 An arbitrary point $X(x, y, z)$ on the plane containing the point $P(2, 3, 4)$ with normal $\mathbf{n} = (1, 2, -1)$

Now

$$\begin{aligned}\overrightarrow{PX} &= \mathbf{x} - \mathbf{p} \quad \text{(where } \mathbf{x} \text{ and } \mathbf{p} \text{ are the position vectors of } X \text{ and } P\text{)}\\ &= (x, y, z) - (2, 3, 4)\\ &= (x - 2, y - 3, z - 4).\end{aligned}$$

Hence the condition for the point $X(x, y, z)$ to lie in the plane is

$$(x - 2, y - 3, z - 4) \cdot (1, 2, -1) = 0,$$

that is,

$$(x - 2) \times 1 + (y - 3) \times 2 + (z - 4) \times (-1) = 0,$$

which simplifies to

$$x + 2y - z = 4.$$

This is the equation of the plane.

In fact every plane in $\mathbb{R}^3$ has an equation of the form

$$ax + by + cz = d,$$

for some real numbers a, b, c and d. To prove this, we apply the argument above to a general plane. Consider the plane that contains the point $P(x_1, y_1, z_1)$ and has $\mathbf{n} = (a, b, c)$ as a normal vector, as illustrated in Figure 77.

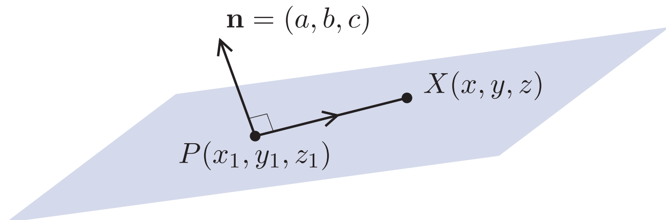


Figure 77 An arbitrary point $X(x, y, z)$ on the plane containing the point $P(x_1, y_1, z_1)$ with normal $\mathbf{n} = (a, b, c)$

A condition for an arbitrary point $X(x, y, z)$ in $\mathbb{R}^3$ to lie in this plane is that the vectors $\overrightarrow{PX}$ and $\mathbf{n}$ must be perpendicular, that is,

$$\overrightarrow{PX} \cdot \mathbf{n} = 0.$$

Since $\overrightarrow{PX} = \mathbf{x} - \mathbf{p}$, where $\mathbf{x}$ and $\mathbf{p}$ are the position vectors of X and P, respectively, this condition can be written as

$$(\mathbf{x} - \mathbf{p}) \cdot \mathbf{n} = 0.$$

By the algebraic properties of the scalar product, we can write the condition as

$$\mathbf{x} \cdot \mathbf{n} - \mathbf{p} \cdot \mathbf{n} = 0,$$

that is,

$$\mathbf{x} \cdot \mathbf{n} = \mathbf{p} \cdot \mathbf{n}.$$

This is the vector form of the equation of the plane. Alternatively, we can write it in terms of the coordinates x, y and z, by substituting for $\mathbf{x} = (x, y, z)$, $\mathbf{n} = (a, b, c)$ and $\mathbf{p} = (x_1, y_1, z_1)$. Then the equation becomes

$$(x, y, z) \cdot (a, b, c) = (x_1, y_1, z_1) \cdot (a, b, c),$$

that is,

$$ax + by + cz = ax_1 + by_1 + cz_1.$$

This equation is of the form

$$ax + by + cz = d,$$

where d is the real number given by $d = ax_1 + by_1 + cz_1$. So we have shown that every plane in $\mathbb{R}^3$ has an equation of this form, for some real numbers a, b, c and d.

Equation of a plane in $\mathbb{R}^3$

The equation of the plane that contains the point (x_1, y_1, z_1) and has the vector $\mathbf{n} = (a, b, c)$ as a normal is

$$ax + by + cz = d,$$

where $d = ax_1 + by_1 + cz_1$.

This equation can be written in vector form as

$$\mathbf{x} \cdot \mathbf{n} = \mathbf{p} \cdot \mathbf{n},$$

where $\mathbf{x} = (x, y, z)$ and $\mathbf{p} = (x_1, y_1, z_1)$.

Once we know the equation of a plane in the form $ax + by + cz = d$, we can 'read off' the components of a normal vector, as they are the coefficients of x, y and z in the equation. For instance, one normal to the plane with equation $x - 2y + 3z = 7$ is $\mathbf{n} = (1, -2, 3)$. Note that the zero vector can never be a normal since its direction is undefined.

When we want to find the equation of a plane, it is simpler to start from the vector form of the equation, as demonstrated in the next worked exercise.

Worked Exercise A23

Determine the equation of the plane in $\mathbb{R}^3$ that contains the point $(1, -1, 4)$ and has the vector $(2, -2, 3)$ as a normal.

Solution

The equation of the plane is

$$\mathbf{x} \cdot \mathbf{n} = \mathbf{p} \cdot \mathbf{n},$$

where $\mathbf{x} = (x, y, z)$, $\mathbf{p} = (1, -1, 4)$ and $\mathbf{n} = (2, -2, 3)$. So the equation of the plane is

$$(x, y, z) \cdot (2, -2, 3) = (1, -1, 4) \cdot (2, -2, 3),$$

that is,

$$2x - 2y + 3z = 1 \times 2 + (-1) \times (-2) + 4 \times 3,$$

which simplifies to

$$2x - 2y + 3z = 16.$$

Exercise A56

Determine the equation of each of the following planes.

(a) The plane that contains the point $(1, 0, 2)$ and has the vector $(2, 3, 1)$ as a normal.

(b) The plane that contains the point $(-1, 1, 5)$ and has the vector $(4, -2, 1)$ as a normal.

In Book C you will see how you can find the equation of a plane in $\mathbb{R}^3$ if you know three points on the plane, rather than a point and a normal.

Summary

In this unit you have studied some fundamental ideas in mathematics. You have met a new notation for specifying sets and encountered examples of sets of numbers and sets of points. You have studied the operations of union, intersection and difference that can be performed on sets, and seen how to show that two sets are equal. You have also met many examples of functions between sets, and seen that a one-to-one function has an inverse. Finally, you have worked with vectors and seen how to carry out vector arithmetic in component form and use the scalar product of two vectors.

Throughout the unit you have worked especially with the sets $\mathbb{R}$, $\mathbb{R}^2$ and $\mathbb{R}^3$, of real numbers, ordered pairs of real numbers and ordered triples of real numbers, respectively. You have seen that the elements of these sets can be regarded geometrically as points on the real line, in the plane and in space, and that points in $\mathbb{R}^2$ or $\mathbb{R}^3$ can also be identified with their position vectors.

You will continue your study of foundational mathematical concepts in the rest of Book A, and the ideas you meet here will be in constant use throughout this module.

Learning outcomes

After working through this unit, you should be able to:

- recognise the *equation of a line* and the *equation of a circle* in $\mathbb{R}^2$
- use *set notation* and the notation of *intervals* of the real line
- determine whether one set is a subset of another, and whether two sets are equal
- find the *union*, *intersection* and *difference* of two sets
- define a *function* and its *domain*, *codomain* and *rule*
- determine the *image set* of a function
- determine whether a function is *one-to-one* and/or *onto*
- find the *inverse* of a one-to-one function, and the *composite* of two functions
- explain what are meant by a *vector*, a *scalar*, a *scalar multiple* of a vector, and the *sum* and *difference* of two vectors
- represent vectors in $\mathbb{R}^2$ and $\mathbb{R}^3$ in terms of their *components*, and carry out vector arithmetic using components
- determine the equation of a line in $\mathbb{R}^2$ or $\mathbb{R}^3$ in terms of vectors
- explain what is meant by the *scalar product* of two vectors, and use it to find the angle between two vectors
- recognise the *equation of a plane* in $\mathbb{R}^3$, and the vector form of the equation
- determine the equation of a plane in $\mathbb{R}^3$, given a point in the plane and a *normal* to the plane.

Solutions to exercises

Solution to Exercise A1

Using the formula for the equation of a line when given its gradient and one point on it, we find that the equation of this line is

$$y - (-1) = -3(x - 2).$$

We can rearrange this to

$$y = -3x + 5,$$

or

$$3x + y = 5.$$

Solution to Exercise A2

(a) Since $(1, 1)$ and $(3, 5)$ lie on the line, its gradient is

$$m = \frac{1-5}{1-3} = 2.$$

Then, since the point $(1, 1)$ lies on the line, its equation must be

$$y - 1 = 2(x - 1),$$

so

$$y = 2x - 1, \text{ or } \quad 2x - y = 1.$$

(b) Both these points have x-coordinate 0, so they lie on the line with equation $x = 0$, the y-axis.

(c) Since the origin lies on the line, its equation must be of the form $y = mx$, where m is its gradient.

Since $(4, 2)$ lies on the line, its coordinates must satisfy the equation of the line. Thus $2 = 4m$, so $m = \frac{1}{2}$.

Hence the equation of this line is $y = \frac{1}{2}x$, or $\frac{1}{2}x - y = 0$, or $x - 2y = 0$.

(d) Both these points have y-coordinate -1, so they lie on the line with equation $y = -1$.

Solution to Exercise A3

We can rearrange the equations of the lines to find their gradients as follows:

$$\begin{array}{ll} l_1: \; y = -2x + 4 & l_2: \; y = 2x + \frac{4}{3} \\ l_3: \; y = -\frac{1}{2}x + 5 & l_4: \; y = \frac{1}{2}x - \frac{5}{6} \\ l_5: \; y = \frac{1}{2}x + 1 & l_6: \; y = -2x - \frac{7}{2} \end{array}$$

Thus the gradients of the given lines are -2, 2, $-\frac{1}{2}$, $\frac{1}{2}$, $\frac{1}{2}$ and -2, respectively.

It follows that the lines l_1 and l_6 are parallel, since their gradients are the same but their y-intercepts are different. Similarly, l_4 and l_5 are also parallel.

Lines l_1 and l_4 are perpendicular, since the product of their gradients is -1. For the same reason, each of the following pairs of lines are perpendicular: l_1 and l_5; l_2 and l_3; l_4 and l_6; and l_5 and l_6.

Solution to Exercise A4

We use the formula for the distance between two points in the plane. This gives the following distances.

(a) $\sqrt{(5-0)^2 + (0-0)^2} = 5$

(b) $\sqrt{(3-0)^2 + (4-0)^2} = 5$

(c) $\sqrt{(5-1)^2 + (1-2)^2} = \sqrt{17}$

(d) $\sqrt{(-1-3)^2 + (4-(-8))^2} = \sqrt{160}$
$= 4\sqrt{10}$

(The two points in part (a) are on the x-axis, so in fact there is no need to use the distance formula to find the distance between them.)

Solution to Exercise A5

(a) This circle has equation

$$(x - 0)^2 + (y - 0)^2 = 4^2,$$

which can be simplified to give

$$x^2 + y^2 = 16.$$

(b) This circle has equation

$$(x - (-1))^2 + (y - 0)^2 = (\sqrt{2})^2,$$

which can be simplified to give

$$(x + 1)^2 + y^2 = 2.$$

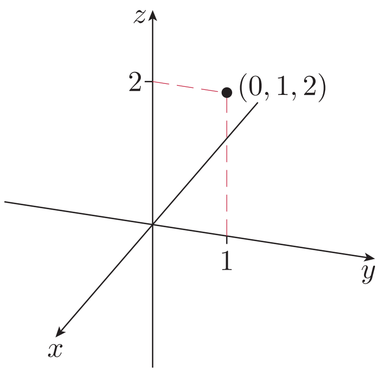
(c) This circle has equation

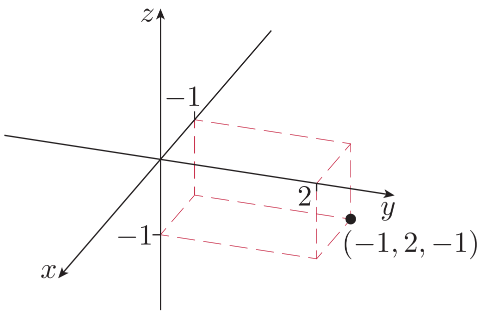
$$(x - 3)^2 + (y - (-4))^2 = 2^2,$$

which can be simplified to give

$$(x - 3)^2 + (y + 4)^2 = 4.$$

Solution to Exercise A6





Solution to Exercise A7

We use the formula for the distance between two points in $\mathbb{R}^3$. This gives the following distances.

(a) $\sqrt{(4-1)^2+(1-1)^2+(-3-1)^2}$
$= \sqrt{9+0+16} = 5$

(b) $\sqrt{(3-1)^2+(0-2)^2+(3-3)^2}$
$= \sqrt{4+4+0} = 2\sqrt{2}$

Solution to Exercise A8

(a) True: -3 is an integer.

(b) False: 5 is a natural number.

(c) False: 1.3 is the rational number $\frac{13}{10}$.

(d) True: both 1 and 3 are rational numbers.

(e) True: $-\pi$ is a real number.

(f) False: $\frac{1}{2}$ is not a natural number.

(g) False: 1 is a non-zero real number, but 0 is not.

(h) False: $\sqrt{2}$ is a real number.

Solution to Exercise A9

(a) True: 1 is a member of the given set.

(b) True: the set $\{-9\}$ is a member of the given set, although the number -9 is not.

(c) False: the number 9 belongs to the given set, but the set $\{9\}$ does not.

(d) False: the point $(0, 1)$ is not a member of the given set of points in $\mathbb{R}^2$, although the point $(1, 0)$ is.

(e) False: the numbers 1 and 0 are not members of the given set of points in $\mathbb{R}^2$, although the point $(1, 0)$ is.

(f) True: the set $\{1, 0\}$ is the same as the set $\{0, 1\}$, and so is a member of the given set. Notice that the members of this set are themselves *sets*, and not points in $\mathbb{R}^2$.

Solution to Exercise A10

(a) True: $\frac{9}{2}$ is in $\mathbb{R}$, and it satisfies the condition $x > 3$.

(b) True: $7 = 3 \times 2 + 1$, so 7 is of the form $3k + 1$ for some $k \in \mathbb{Z}$.

(c) False: $-\frac{7}{2}$ is not in $\mathbb{Z}$.

(d) False: 8 cannot be expressed as 2^x for some number $x \in \mathbb{R}$ satisfying $0 < x < 2$; in fact $8 = 2^3$.

(e) True: 9 is in $\mathbb{Z}$, and $9 = 3^2$ so $9 = k^2$ for some $k \in \mathbb{Z}$.

(f) True: $6 = 3(3-1)$, so 6 is of the form $m(m-1)$ for some $m \in \mathbb{N}$.

(g) False: 4 is an even integer, but it does not satisfy $0 < r < 4$.

Solution to Exercise A11

(a) $\{k \in \mathbb{Z} : -2 < k < 1000\}$

(b) $\{x \in \mathbb{Q} : x > 0 \text{ and } x^2 > 2\}$ or $\{x \in \mathbb{Q} : x > 0,\ x^2 > 2\}$

(c) $\{2n : n \in \mathbb{N}\}$

(d) $\{2^k : k \in \mathbb{Z}\}$

Solution to Exercise A12

(a) False: the set $(1,5)$ is an open interval and does not include the endpoint 1.

(b) True: the set $(-1,1]$ is half-open, with the upper endpoint 1 included.

(c) False: ∞ does not denote a number and so is not in the interval.

(d) True: $\mathbb{R}^*$ denotes the set of non-zero real numbers, so 0 is not a member of this set.

(e) False: $x \in \mathbb{R}^*$ means x is a non-zero real number, while $(0,\infty)$ comprises just the positive real numbers. For example, the number -1 is in $\mathbb{R}^*$, but not in $(0,\infty)$.

Solution to Exercise A13

(a) $[-11,2)$

(b) $(-6.5,21]$

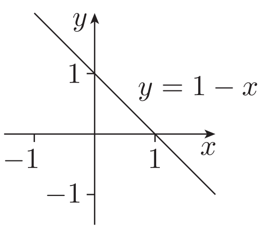
(c) $(-273,\infty)$

Solution to Exercise A14

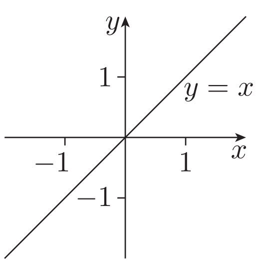
(a) $l = \{(x,y) \in \mathbb{R}^2 : y = 2x+5\}$

(There are other ways to specify this line; another example is $l = \{(x, 2x+5) : x \in \mathbb{R}\}$.)

(b) The line l has equation $y = 1-x$, so it is as follows.



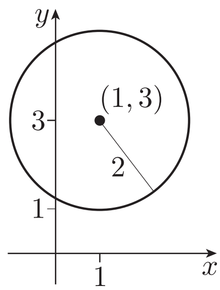
(c) The line l has equation $y = x$ (since here $m = 1$ and $c = 0$), so it is as follows.



Solution to Exercise A15

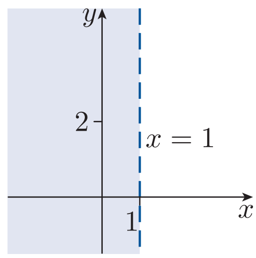
(a) $C = \{(x,y) \in \mathbb{R}^2 : (x-1)^2 + (y+4)^2 = 9\}$

(b) The circle has centre $(1,3)$ and radius 2.

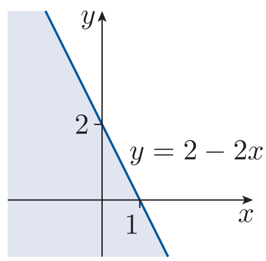


Solution to Exercise A16

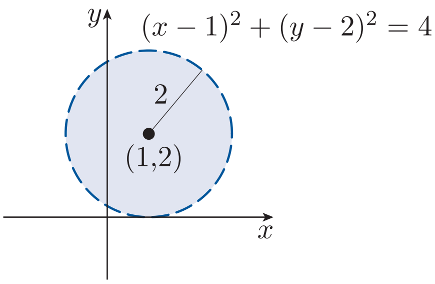
(a) This set is a half-plane with the boundary line excluded, as follows.



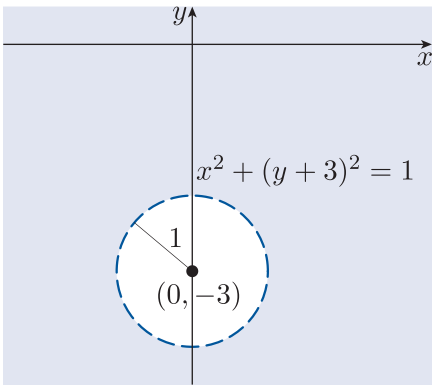
(b) This set is another half-plane, but this time the boundary line is included, as follows.



(c) This set is a disc with the boundary excluded, as follows.

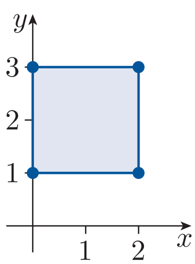


(d) This set consists of the points outside a disc with centre $(0, -3)$ and radius 1, as follows.



Solution to Exercise A17

$\{(x, y) \in \mathbb{R}^2 : 0 \leq x \leq 2,\ 1 \leq y \leq 3\}$



Solution to Exercise A18

(a) The set B consists of the solutions of the equation

$$x^2 + x - 6 = 0,$$

which we can write as

$$(x-2)(x+3) = 0.$$

So $B = \{2, -3\} = A$.

(b) The two sets are

$$\begin{aligned} A &= \{k \in \mathbb{Z} : k \text{ is odd and } 0 < k < 8\} \\ &= \{1, 3, 5, 7\}, \\ B &= \{2n+1 : n \in \mathbb{N} \text{ and } n^2 < 25\} \\ &= \{3, 5, 7, 9\}. \end{aligned}$$

Hence $A \neq B$, either because $9 \in B$ but $9 \notin A$, or because $1 \in A$ but $1 \notin B$.

Solution to Exercise A19

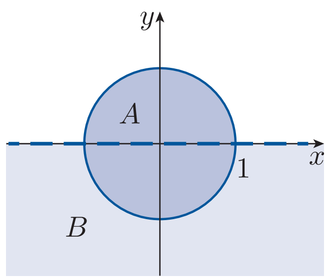
(a) Each element of A is a point in $\mathbb{R}^2$.

We calculate $x - 4y$ using the coordinates of each point of A:

$$\begin{aligned} 5 - 4 \times 2 &= -3, \\ 1 - 4 \times 1 &= -3, \\ -3 - 4 \times 0 &= -3. \end{aligned}$$

This shows that each element of A is an element of B, so $A \subseteq B$.

(b) The sets A and B are sketched below.



The set A is the interior of the unit circle, and B is the half-plane consisting of all points with negative y-coordinate. So $A \nsubseteq B$, because, for example, the point $\left(\frac{1}{2}, \frac{1}{2}\right)$ belongs to A but not to B. (Any one point that is in set A but not in set B shows that $A \nsubseteq B$.)

(c) Let x be an arbitrary element of A; then $x \in \mathbb{R}$ and satisfies $-1 \leq x \leq 0$. This equation gives

$$-1 + 1 \leq x + 1 \leq 0 + 1,$$

that is,

$$0 \leq x + 1 \leq 1.$$

Hence

$$0 \leq (x+1)^2 \leq 1,$$

so $x \in B$.

Since x is an arbitrary element of A, we conclude that $A \subseteq B$.

Solution to Exercise A20

(a) We showed that $A \subseteq B$ in the solution to Exercise A19(a). Also, for example, the point $(9, 3)$ lies in B, since

$$9 - 4 \times 3 = -3,$$

but does not lie in A. Therefore A is a proper subset of B.

(b) We showed that $A \subseteq B$ in the solution to Exercise A19(c). Also, for example, -2 lies in B, since

$$(-2+1)^2 = (-1)^2 = 1,$$

but does not lie in A. Therefore A is a proper subset of B.

Solution to Exercise A21

(a) First we show that $A \subseteq B$.

Let $(x, y) \in A$; then $(x, y) \in \mathbb{R}^2$, and for some $t \in \mathbb{R}$, we have $x = t^2$ and $y = 2t$. Hence

$$y^2 = (2t)^2 = 4t^2 = 4x.$$

So $(x, y) \in B$, and $A \subseteq B$.

Next we show that $B \subseteq A$.

Let $(x, y) \in B$; then $y^2 = 4x$. We must show that there is a value of t in $\mathbb{R}$ such that $x = t^2$ and $y = 2t$, so that $(x, y) \in A$. Let t be given by $y = 2t$; that is, $t = \frac{1}{2}y$. Then, since $4x = y^2$, we have $x = \frac{1}{4}y^2$, and substituting for y gives

$$x = \frac{1}{4}(2t)^2 = t^2.$$

Hence $(x, y) = (t^2, 2t) \in A$, and so $B \subseteq A$.

Since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$.

(b) First we show that $A \subseteq B$.

Let $(x, y) \in A$; then $2x + y - 3 = 0$. We must show that there is a value of t in $\mathbb{R}$ such that $x = t + 1$ and $y = 1 - 2t$. Let t be given by $x = t + 1$, that is, $t = x - 1$. Then, since $2x + y - 3 = 0$, we have

$$\begin{aligned} y &= 3 - 2x \\ &= 3 - 2(t+1) \\ &= 1 - 2t. \end{aligned}$$

Hence $(x, y) = (t + 1, 1 - 2t) \in B$, and so $A \subseteq B$.

Next we show that $B \subseteq A$.

Let $(x, y) \in B$; then $(x, y) \in \mathbb{R}^2$, and for some $t \in \mathbb{R}$, we have $x = t + 1$ and $y = 1 - 2t$. We must show that (x, y) satisfies $2x + y - 3 = 0$. Now

$$\begin{aligned} 2x + y - 3 &= 2(t+1) + (1-2t) - 3 \\ &= 0, \end{aligned}$$

as required, so $(x, y) \in A$. Therefore $B \subseteq A$.

Since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$.

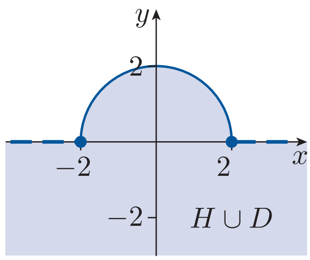
Solution to Exercise A22

(a) $(1, 7) \cup [4, 11] = (1, 11]$.

(b) $\mathbb{R}^*$ denotes the set of non-zero real numbers, and so is the union of the two intervals $(-\infty, 0)$ and $(0, \infty)$; that is

$$\mathbb{R}^* = (-\infty, 0) \cup (0, \infty).$$

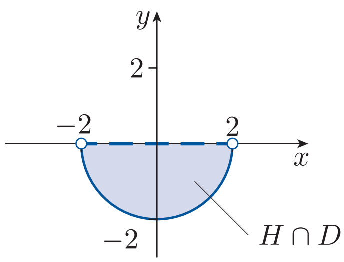
(c) The union of the half-plane and disc is



Solution to Exercise A23

(a) $(1, 7) \cap [4, 11] = [4, 7)$.

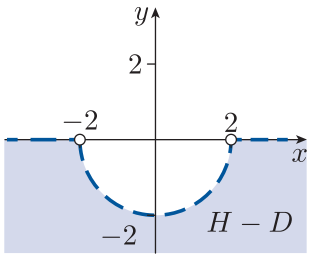
(b) The intersection is

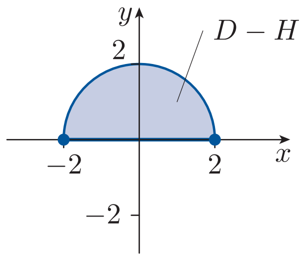


Solution to Exercise A24

(a) $(1, 7) - [4, 11] = (1, 4)$ and $[4, 11] - (1, 7) = [7, 11]$.

(b) The two differences are





Solution to Exercise A25

(a) This is the translation of the plane that moves each point to the right by 2 units and up by 3 units.

(b) This is the reflection of the plane in the x-axis.

(c) This is the rotation of the plane through $\pi/2$ anticlockwise about the origin.

Solution to Exercise A26

Only diagram (b) represents a function.

Diagram (a) does not represent a function, as there is no arrow from the element 3.

Diagram (c) does not represent a function, as there are two arrows from the element 1.

Solution to Exercise A27

(a) $$\begin{aligned} f(S) &= \{f(0), f(1), f(2), f(3)\} \\ &= \{-1, 0, 1, 2\}. \end{aligned}$$

(b) $$\begin{aligned} f(\mathbb{Z}) &= \{\dots, f(-1), f(0), f(1), f(2), \dots\} \\ &= \{\dots, -2, -1, 0, 1 \dots\} \\ &= \mathbb{Z}. \end{aligned}$$

Solution to Exercise A28

The images of the elements of A are
$f(0) = 9,\ f(1) = 8,\ f(2) = 7,\ f(3) = 6,$
$f(4) = 5,\ f(5) = 4,\ f(6) = 3,\ f(7) = 2,$
$f(8) = 1,\ f(9) = 0.$

So the image set of f is
$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = A$.

Solution to Exercise A29

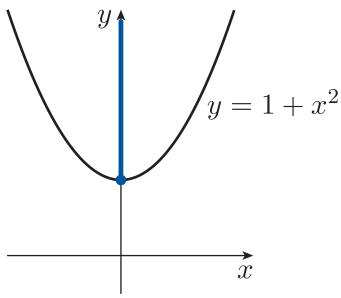
Only diagram (a) represents an onto function.

Diagram (b) does not even represent a function, as there is no arrow from the element 4.

Diagram (c) represents a function that is not onto, as there is no arrow going to the element 1.

Solution to Exercise A30

(a) The sketch of the graph of f below suggests that $f(\mathbb{R}) = [1, \infty)$.



We prove that $f(\mathbb{R}) = [1, \infty)$.

Let $x \in \mathbb{R}$; then $f(x) = 1 + x^2$. Since $x^2 \geq 0$, we have $1 + x^2 \geq 1$ and so $f(\mathbb{R}) \subseteq [1, \infty)$.

We must show that $f(\mathbb{R}) \supseteq [1, \infty)$.

Let $y \in [1, \infty)$. We must show that there exists $x \in \mathbb{R}$ such that $f(x) = y$; that is, $1 + x^2 = y$. Now $x = \sqrt{y-1}$ is real, since $y \geq 1$, and satisfies $f(x) = y$, as required. (Alternatively, $x = -\sqrt{y-1}$ is real and satisfies $f(x) = y$.)

Thus $f(\mathbb{R}) \supseteq [1, \infty)$.

Since $f(\mathbb{R}) \subseteq [1, \infty)$ and $f(\mathbb{R}) \supseteq [1, \infty)$, it follows that $f(\mathbb{R}) = [1, \infty)$, so the image set of f is $[1, \infty)$, as expected.

The interval $[1, \infty)$ is not the whole of the codomain $\mathbb{R}$, so f is not onto.

(b) This function is the reflection of the plane in the x-axis. This suggests that $f(\mathbb{R}^2) = \mathbb{R}^2$.

We know that $f(\mathbb{R}^2) \subseteq \mathbb{R}^2$, so we must show that $f(\mathbb{R}^2) \supseteq \mathbb{R}^2$.

Let $(x', y') \in \mathbb{R}^2$. We must show that there exists $(x, y) \in \mathbb{R}^2$ such that $f(x, y) = (x', y')$; so $(x, -y) = (x', y')$, that is,

$$x = x', \quad -y = y'.$$

Rearranging these equations, we obtain

$$x = x', \quad y = -y'.$$

So, $(x, y) \in \mathbb{R}^2$ and $f(x, y) = (x', y')$, as required.

Thus $f(\mathbb{R}^2) \supseteq \mathbb{R}^2$.

Since $f(\mathbb{R}^2) \subseteq \mathbb{R}^2$ and $f(\mathbb{R}^2) \supseteq \mathbb{R}^2$, it follows that $f(\mathbb{R}^2) = \mathbb{R}^2$, so the image set of f is $\mathbb{R}^2$, as expected.

The codomain of f is also $\mathbb{R}^2$, so f is onto.

Solution to Exercise A31

Only diagram (c) represents a one-to-one function.

Diagram (a) represents a function that is not one-to-one, as there are two arrows going to the element 3.

Diagram (b) does not even represent a function, as there is no arrow from the element 2.

Solution to Exercise A32

(a) This function is not one-to-one since, for example,

$$f(2) = f(-2) = 1 + 4 = 5.$$

(b) This function is the reflection of the plane in the x-axis, so we expect it to be one-to-one. We now prove this algebraically.

Suppose that $f(x_1, y_1) = f(x_2, y_2)$; then

$$(x_1, -y_1) = (x_2, -y_2).$$

This means that $x_1 = x_2$ and $-y_1 = -y_2$,. It follows that $y_1 = y_2$, so we have shown that $(x_1, y_1) = (x_2, y_2)$, that is, f is one-to-one.

Solution to Exercise A33

(a) In Exercise A32 we saw that f is not one-to-one, so f does not have an inverse function.

(b) In Exercise A32 we saw that f is one-to-one, so f has an inverse function.

In Exercise A30 we saw that the image set of f is $\mathbb{R}^2$ and, for each $(x', y') \in \mathbb{R}^2$, we have

$$(x', y') = f(x', -y').$$

So f^{-1} is the function

$$\begin{aligned} f^{-1} : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x', y') &\longmapsto (x', -y'). \end{aligned}$$

This can be expressed in terms of x and y as

$$\begin{aligned} f^{-1} : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x, -y). \end{aligned}$$

(In this case, f^{-1} is actually equal to f, which is what we would expect for a reflection.)

(c) The graph of this function is an upward sloping straight line, which suggests that it is one-to-one. First we confirm this algebraically. Suppose that $f(x_1) = f(x_2)$; then

$$8x_1 + 3 = 8x_2 + 3,$$

so $8x_1 = 8x_2$, and hence $x_1 = x_2$. Thus f is one-to-one, and so it has an inverse function.

We now find the image set of f. We suspect that its image set is $\mathbb{R}$, so we now prove this algebraically. Let y be an arbitrary element in $\mathbb{R}$. We must show that there exists an element x in the domain $\mathbb{R}$ such that

$$f(x) = y; \quad \text{that is,} \quad 8x + 3 = y.$$

Rearranging this equation, we obtain

$$x = \frac{y - 3}{8}.$$

This is in $\mathbb{R}$ and satisfies $f(x) = y$, as required. Thus the image set of f is $\mathbb{R}$.

Hence f^{-1} is the function

$$\begin{aligned} f^{-1} : \mathbb{R} &\longrightarrow \mathbb{R} \\ y &\longmapsto \frac{y - 3}{8}. \end{aligned}$$

This can be expressed in terms of x as

$$\begin{aligned} f^{-1} : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{x - 3}{8}. \end{aligned}$$

Solution to Exercise A34

The function

$$\begin{aligned} g : [-\pi/2, \pi/2] &\longrightarrow [-1, 1] \\ x &\longmapsto \sin x \end{aligned}$$

is a restriction of f that is one-to-one.

(There are many other possibilities, for example, the restriction of the domain to $[\pi/2, 3\pi/2]$.)

Solution to Exercise A35

(a) The rule of $g \circ f$ is

$$\begin{aligned}(g \circ f)(x) = g(f(x)) &= g(-x)\\ &= 3(-x) + 1\\ &= -3x + 1.\end{aligned}$$

Thus $g \circ f$ is the function

$$\begin{aligned}g \circ f : \mathbb{R} &\longrightarrow \mathbb{R}\\ x &\longmapsto -3x + 1.\end{aligned}$$

(b) The rule of $f \circ g$ is

$$\begin{aligned}(f \circ g)(x) = f(g(x)) &= f(3x + 1)\\ &= -(3x + 1)\\ &= -3x - 1.\end{aligned}$$

Thus $f \circ g$ is the function

$$\begin{aligned}f \circ g : \mathbb{R} &\longrightarrow \mathbb{R}\\ x &\longmapsto -3x - 1.\end{aligned}$$

Solution to Exercise A36

The rule of $f \circ g$ is

$$\begin{aligned}(f \circ g)(x, y) = f(g(x, y)) &= f(-x, y)\\ &= (-x, -y).\end{aligned}$$

Thus $f \circ g$ is the function

$$\begin{aligned}f \circ g : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2\\ (x, y) &\longmapsto (-x, -y).\end{aligned}$$

(In this case, $f \circ g = g \circ f$.)

Solution to Exercise A37

The rule of $g \circ f$ is

$$\begin{aligned}(g \circ f)(x) = g(f(x)) &= g(3x + 1)\\ &= \frac{3}{(3x + 1) + 2}\\ &= \frac{1}{x + 1}.\end{aligned}$$

The domain of $g \circ f$ is

$$\{x \in [-1, 1] : f(x) \in \mathbb{R} - \{-2\}\}.$$

If $x \in [-1, 1]$, then $f(x) \in \mathbb{R} - \{-2\}$ unless $f(x) = -2$. Now $f(x) = -2$ when

$$3x + 1 = -2,$$

that is, when

$$x = -1.$$

So the domain of $g \circ f$ is

$$[-1, 1] - \{-1\} = (-1, 1].$$

Thus $g \circ f$ is the function

$$\begin{aligned}g \circ f : (-1, 1] &\longrightarrow \mathbb{R}\\ x &\longmapsto \frac{1}{x + 1}.\end{aligned}$$

Solution to Exercise A38

The domain of f is $\mathbb{R}$, and for each $x \in \mathbb{R}$ we have

$$g(f(x)) = g\,(5x - 3) = \frac{(5x - 3) + 3}{5} = x;$$

that is, $g \circ f = i_{\mathbb{R}}$.

The domain of g is also $\mathbb{R}$, and for each $y \in \mathbb{R}$ we have

$$f(g(y)) = f\left(\frac{y + 3}{5}\right) = 5\left(\frac{y + 3}{5}\right) - 3 = y;$$

that is, $f \circ g = i_{\mathbb{R}}$.

Since $g \circ f = i_{\mathbb{R}}$ and $f \circ g = i_{\mathbb{R}}$, it follows that g is the inverse function of f.

Solution to Exercise A39

This is a translation of the plane that shifts each point to the left by 1 unit and up by 3 units, so we expect its inverse to shift the plane to the right by 1 unit and down by 3 units.

Let

$$\begin{aligned}g : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2\\ (x, y) &\longmapsto (x + 1, y - 3).\end{aligned}$$

The domain of f is $\mathbb{R}^2$, and for each $(x, y) \in \mathbb{R}^2$ we have

$$\begin{aligned}g(f(x, y)) &= g(x - 1, y + 3)\\ &= (x - 1 + 1, y + 3 - 3)\\ &= (x, y);\end{aligned}$$

that is, $g \circ f = i_{\mathbb{R}^2}$.

The domain of g is also $\mathbb{R}^2$, and for each $(x, y) \in \mathbb{R}^2$ we have

$$\begin{aligned}f(g(x, y)) &= f(x + 1, y - 3)\\ &= (x + 1 - 1, y - 3 + 3)\\ &= (x, y);\end{aligned}$$

that is, $f \circ g = i_{\mathbb{R}^2}$.

Since $g \circ f = i_{\mathbb{R}^2}$ and $f \circ g = i_{\mathbb{R}^2}$, it follows that g is the inverse function of f.

Solution to Exercise A40

The vector $\mathbf{d}$ is in the same direction as $\mathbf{a}$, but none of the other vectors is; also, the magnitude of $\mathbf{d}$ is two-thirds that of $\mathbf{a}$. Hence

$$\mathbf{d} = \tfrac{2}{3}\mathbf{a} \quad \text{and} \quad \mathbf{a} = \tfrac{3}{2}\mathbf{d}.$$

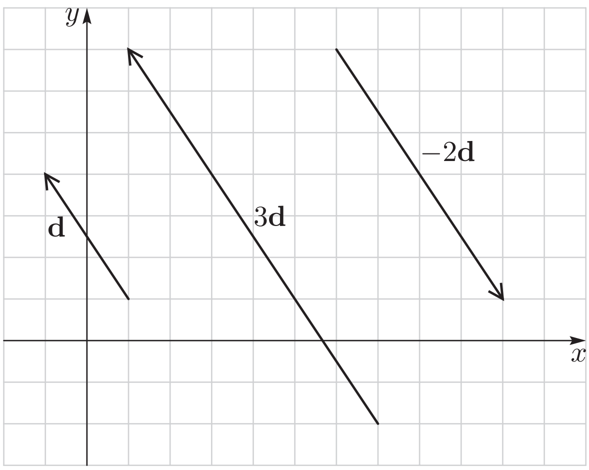
Next, $\mathbf{e}$ is parallel to $\mathbf{b}$ but in the opposite direction; none of the others is parallel to these two vectors. Also, the magnitude of $\mathbf{e}$ is three times that of $\mathbf{b}$. Hence

$$\mathbf{e} = -3\mathbf{b} \quad \text{and} \quad \mathbf{b} = -\tfrac{1}{3}\mathbf{e}.$$

Finally, $\mathbf{c}$ and $\mathbf{f}$ are not multiples of any of the other vectors.

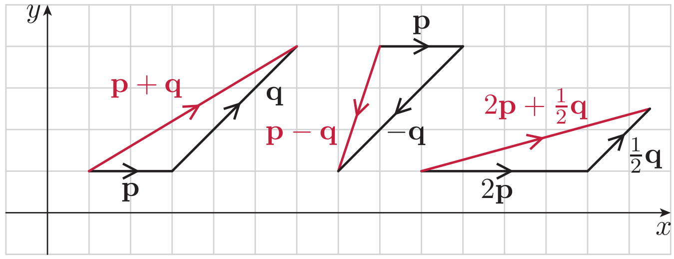
Solution to Exercise A41

The vector $3\mathbf{d}$ is in the same direction as $\mathbf{d}$, but its magnitude is three times that of $\mathbf{d}$; the vector $-2\mathbf{d}$ is in the opposite direction to that of $\mathbf{d}$, and its magnitude is twice that of $\mathbf{d}$.

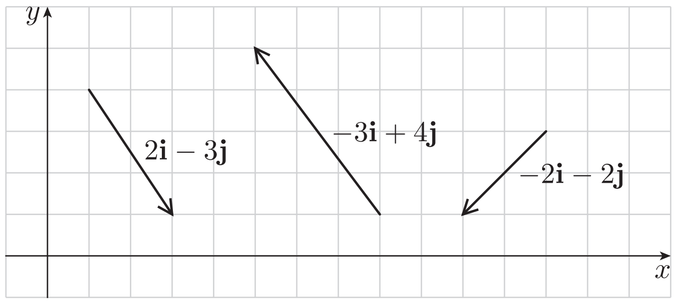


Solution to Exercise A42

We use the rule for forming a scalar multiple of a vector, and the Triangle Law for the addition of vectors.



Solution to Exercise A43



Solution to Exercise A44

(a) Here $\mathbf{p} = (3, -1)$ and $\mathbf{q} = (-1, -2)$, so

$$\begin{aligned}\mathbf{p}+\mathbf{q} &= (3+(-1), -1+(-2)) = (2,-3),\\ -\mathbf{q} &= (1,2),\\ \mathbf{p}-\mathbf{q} &= (3-(-1), -1-(-2)) = (4,1).\end{aligned}$$

(b) Here $\mathbf{p} = -\mathbf{i} - 2\mathbf{j}$ and $\mathbf{q} = 2\mathbf{i} - \mathbf{j}$, so

$$\begin{aligned}\mathbf{p}+\mathbf{q} &= (-1+2)\mathbf{i} + (-2+(-1))\mathbf{j} = \mathbf{i} - 3\mathbf{j},\\ -\mathbf{q} &= -2\mathbf{i} + \mathbf{j},\\ \mathbf{p}-\mathbf{q} &= (-1-2)\mathbf{i} + (-2-(-1))\mathbf{j} = -3\mathbf{i} - \mathbf{j}.\end{aligned}$$

(c) Here $\mathbf{p} = -\mathbf{i} + 2\mathbf{k}$ and $\mathbf{q} = \mathbf{i} - 2\mathbf{j} - \mathbf{k}$, so

$$\begin{aligned}\mathbf{p}+\mathbf{q} &= (-1+1)\mathbf{i} - 2\mathbf{j} + (2-1)\mathbf{k} = -2\mathbf{j} + \mathbf{k},\\ -\mathbf{q} &= -\mathbf{i} + 2\mathbf{j} + \mathbf{k},\\ \mathbf{p}-\mathbf{q} &= (-1-1)\mathbf{i} - (-2\mathbf{j}) + (2-(-1))\mathbf{k},\\ &= -2\mathbf{i} + 2\mathbf{j} + 3\mathbf{k}.\end{aligned}$$

Solution to Exercise A45

(a) Since $\mathbf{p} = (3, -1)$ and $\mathbf{q} = (-1, -2)$,

$$2\mathbf{p} = (6, -2),$$
$$3\mathbf{q} = (-3, -6),$$
$$2\mathbf{p} - 3\mathbf{q} = (9, 4).$$

The magnitude of $\mathbf{q}$ is

$$|\mathbf{q}| = \sqrt{(-1)^2 + (-2)^2} = \sqrt{5}.$$

(b) Since $\mathbf{p} = -\mathbf{i} + 2\mathbf{k}$ and $\mathbf{q} = \mathbf{i} - 2\mathbf{j} - \mathbf{k}$,

$$2\mathbf{p} = -2\mathbf{i} + 4\mathbf{k},$$
$$3\mathbf{q} = 3\mathbf{i} - 6\mathbf{j} - 3\mathbf{k},$$
$$2\mathbf{p} - 3\mathbf{q} = -5\mathbf{i} + 6\mathbf{j} + 7\mathbf{k}.$$

The magnitude of $\mathbf{q}$ is

$$|\mathbf{q}| = \sqrt{(1)^2 + (-2)^2 + (-1)^2} = \sqrt{6}.$$

Solution to Exercise A46

(a) When $\mathbf{v} = (2, -3)$, the magnitude of $\mathbf{v}$ is

$$|\mathbf{v} = \sqrt{2^2 + (-3)^2} = \sqrt{4 + 9} = \sqrt{13},$$

so

$$\widehat{\mathbf{v}} = \frac{1}{\sqrt{13}}(2, -3) = \left(\frac{2}{\sqrt{13}}, -\frac{3}{\sqrt{13}}\right).$$

(b) When $\mathbf{v} = 5\mathbf{i} + 12\mathbf{j}$, the magnitude of $\mathbf{v}$ is

$$|\mathbf{v}| = \sqrt{5^2 + 12^2} = \sqrt{25 + 144} = 13,$$

so

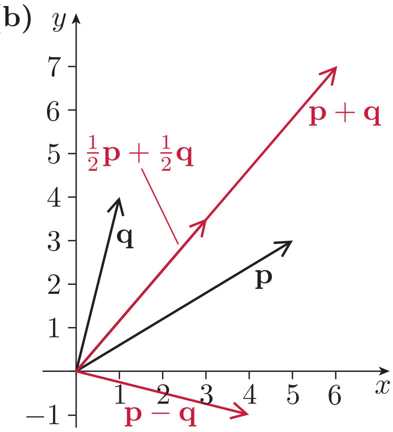
$$\widehat{\mathbf{v}} = \frac{1}{|\mathbf{v}|}\mathbf{v} = \frac{5}{13}\mathbf{i} + \frac{12}{13}\mathbf{j}.$$

Solution to Exercise A47

(a) Since $\mathbf{p} = (5, 3)$ and $\mathbf{q} = (1, 4)$,

$$\mathbf{p} - \mathbf{q} = (4, -1),$$
$$\mathbf{p} + \mathbf{q} = (6, 7),$$
$$\tfrac{1}{2}\mathbf{p} + \tfrac{1}{2}\mathbf{q} = \left(\tfrac{5}{2}, \tfrac{3}{2}\right) + \left(\tfrac{1}{2}, 2\right) = \left(3, \tfrac{7}{2}\right).$$

(b)



Solution to Exercise A48

(a) The vector form of the equation of l is

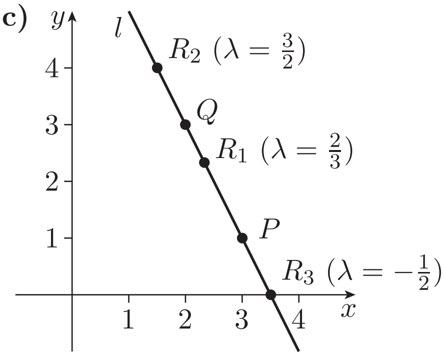
$$\begin{aligned}\mathbf{r} &= (1 - \lambda)(3, 1) + \lambda(2, 3)\\ &= (3 - \lambda, 1 + 2\lambda).\end{aligned}$$

(b) Using the formula above with $\lambda = \frac{2}{3}$, $\frac{3}{2}$ and $-\frac{1}{2}$ in turn, we obtain the following position vectors:

$$\mathbf{r}_1 = \left(3 - \tfrac{2}{3}, 1 + \tfrac{4}{3}\right) = \left(\tfrac{7}{3}, \tfrac{7}{3}\right),$$
$$\mathbf{r}_2 = \left(3 - \tfrac{3}{2}, 1 + 3\right) = \left(\tfrac{3}{2}, 4\right),$$
$$\mathbf{r}_3 = \left(3 - (-\tfrac{1}{2}), 1 + (-1)\right) = \left(\tfrac{7}{2}, 0\right).$$

Thus the three points on the line are the points R_1, R_2 and R_3, with coordinates $\left(\frac{7}{3}, \frac{7}{3}\right)$, $\left(\frac{3}{2}, 4\right)$ and $\left(\frac{7}{2}, 0\right)$, respectively.

(c)



Solution to Exercise A49

(a) The vector form of the equation of l is

$$\mathbf{r} = (3 - \lambda, 1 + 2\lambda).$$

Hence at the point $(4, -1)$ on l, we have

$$(4, -1) = (3 - \lambda, 1 + 2\lambda).$$

Equating the corresponding components gives

$$4 = 3 - \lambda \quad \text{and} \quad -1 = 1 + 2\lambda.$$

The first equation gives $\lambda = -1$, and this value of λ also satisfies the other equation. Hence the value of λ corresponding to the point $(4, -1)$ in the vector form of the equation of l is $\lambda = -1$.

(b) The point $\left(\frac{1}{2}, \frac{1}{2}\right)$ lies on l if and only if there is some real number λ for which

$$\left(\tfrac{1}{2}, \tfrac{1}{2}\right) = (3 - \lambda, 1 + 2\lambda).$$

Equating corresponding components gives

$$3 - \lambda = \tfrac{1}{2} \quad \text{and} \quad 1 + 2\lambda = \tfrac{1}{2}.$$

The first of these equations has solution $\lambda = \frac{5}{2}$, and the second has solution $\lambda = -\frac{1}{4}$.

It follows that there is no real number λ that satisfies the vector form of the equation of l, when $\mathbf{r} = \left(\frac{1}{2}, \frac{1}{2}\right)$, so the point $\left(\frac{1}{2}, \frac{1}{2}\right)$ does not lie on l.

Solution to Exercise A50

(a) The vector form of the equation of the line l is

$$\begin{aligned}\mathbf{r} &= (1-\lambda)(2,1,0) + \lambda(1,0,-1)\\ &= (2-\lambda,\ 1-\lambda,\ -\lambda).\end{aligned}$$

(b) Using the formula above with $\lambda = \frac{1}{2}$ and -1, we obtain the following position vectors:

$$\begin{aligned}\mathbf{r}_1 &= \left(2 - \tfrac{1}{2},\ 1 - \tfrac{1}{2},\ -\tfrac{1}{2}\right)\\ &= \left(\tfrac{3}{2}, \tfrac{1}{2}, -\tfrac{1}{2}\right),\\ \mathbf{r}_2 &= (2-(-1),\ 1-(-1),\ -(-1))\\ &= (3,2,1).\end{aligned}$$

Thus the two points have coordinates $\left(\frac{3}{2}, \frac{1}{2}, -\frac{1}{2}\right)$ and $(3, 2, 1)$.

Solution to Exercise A51

We use the formula for the scalar product of vectors in component form.

(a) $$\begin{aligned}(2,3)\cdot\left(\tfrac{5}{2},-4\right) &= 2\times\tfrac{5}{2} + 3\times(-4)\\ &= 5 - 12 = -7\end{aligned}$$

(b) $$\begin{aligned}(1,4)\cdot\left(2,-\tfrac{1}{2}\right) &= 1\times 2 + 4\times\left(-\tfrac{1}{2}\right)\\ &= 2 - 2 = 0\end{aligned}$$

(c) $$\begin{aligned}&(-2\mathbf{i} + \mathbf{j})\cdot(3\mathbf{i} - 2\mathbf{j})\\ &\qquad = (-2)\times 3 + 1\times(-2)\\ &\qquad = -6 - 2 = -8\end{aligned}$$

(d) $$\begin{aligned}&(1,-1,-2)\cdot(3,-2,-5)\\ &\quad = 1\times 3 + (-1)\times(-2) + (-2)\times(-5)\\ &\quad = 3 + 2 + 10 = 15\end{aligned}$$

Solution to Exercise A52

In each case we let $\mathbf{u}$ denote the first vector of the pair, $\mathbf{v}$ the second vector, and θ the angle between the two vectors.

(a) Here

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} &= (1,4)\cdot(5,2) = 5 + 8 = 13,\\ |\mathbf{u}| &= \sqrt{1^2+4^2} = \sqrt{1+16} = \sqrt{17},\\ |\mathbf{v}| &= \sqrt{5^2+2^2} = \sqrt{25+4} = \sqrt{29}.\end{aligned}$$

Hence

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|} = \frac{13}{\sqrt{17}\sqrt{29}} = \frac{13}{\sqrt{493}},$$

so

$$\begin{aligned}\theta &= \cos^{-1}\left(\frac{13}{\sqrt{493}}\right)\\ &= 0.95 \text{ radians} \quad \text{(to 2 d.p.)}.\end{aligned}$$

(b) Here

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} &= (-2,2)\cdot(1,-1) = -2 - 2 = -4,\\ |\mathbf{u}| &= \sqrt{(-2)^2+2^2} = \sqrt{4+4} = \sqrt{8} = 2\sqrt{2},\\ |\mathbf{v}| &= \sqrt{1^2+(-1)^2} = \sqrt{1+1} = \sqrt{2}.\end{aligned}$$

Hence

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|} = \frac{-4}{2\sqrt{2}\sqrt{2}} = -1,$$

so

$$\theta = \cos^{-1}(-1) = \pi \text{ radians}.$$

You might have expected this result, because $\mathbf{u}$ and $\mathbf{v}$ point in opposite directions (in fact, $\mathbf{u} = -2\mathbf{v}$).

(c) Here

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} &= (9\mathbf{i} - 2\mathbf{j})\cdot(\mathbf{i} + 2\mathbf{j})\\ &= 9\times 1 + (-2)\times 2\\ &= 9 - 4 = 5,\\ |\mathbf{u}| &= \sqrt{9^2+(-2)^2} = \sqrt{81+4} = \sqrt{85},\\ |\mathbf{v}| &= \sqrt{1^2+2^2} = \sqrt{5}.\end{aligned}$$

Hence

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|} = \frac{5}{\sqrt{85}\sqrt{5}} = \frac{1}{\sqrt{17}},$$

so

$$\begin{aligned}\theta &= \cos^{-1}\left(\frac{1}{\sqrt{17}}\right)\\ &= 1.33 \text{ radians} \quad (\text{to 2 d.p.}).\end{aligned}$$

Solution to Exercise A53

In each case we let $\mathbf{u}$ denote the first vector of the pair, $\mathbf{v}$ the second vector, and θ the angle between the two vectors.

(a) Here

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} &= (3,4,5)\cdot(1,0,-1)\\ &= 3\times 1 + 4\times 0 + 5\times(-1) = -2,\end{aligned}$$

$$|\mathbf{u}| = \sqrt{3^2+4^2+5^2} = \sqrt{50} = 5\sqrt{2},$$

$$|\mathbf{v}| = \sqrt{1^2+0^2+(-1)^2} = \sqrt{2}.$$

Hence

$$\begin{aligned}\cos\theta &= \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|}\\ &= \frac{-2}{5\sqrt{2}\sqrt{2}} = -\frac{1}{5},\end{aligned}$$

so

$$\begin{aligned}\theta &= \cos^{-1}\left(-\frac{1}{5}\right)\\ &= 1.77 \text{ radians} \quad (\text{to 2 d.p.}).\end{aligned}$$

(b) Here

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} &= (2\mathbf{j}-3\mathbf{k})\cdot(-\mathbf{i}-\mathbf{j}-2\mathbf{k})\\ &= 0\times(-1) + 2\times(-1) + (-3)\times(-2)\\ &= -2+6 = 4,\end{aligned}$$

$$\begin{aligned}|\mathbf{u}| &= \sqrt{0^2+2^2+(-3)^2}\\ &= \sqrt{4+9} = \sqrt{13}\end{aligned}$$

$$\begin{aligned}|\mathbf{v}| &= \sqrt{(-1)^2+(-1)^2+(-2)^2}\\ &= \sqrt{1+1+4} = \sqrt{6}.\end{aligned}$$

Hence

$$\begin{aligned}\cos\theta &= \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|}\\ &= \frac{4}{\sqrt{13}\sqrt{6}} = \frac{4}{\sqrt{78}},\end{aligned}$$

so

$$\begin{aligned}\theta &= \cos^{-1}\left(\frac{4}{\sqrt{78}}\right)\\ &= 1.10 \text{ radians} \quad (\text{to 2 d.p.}).\end{aligned}$$

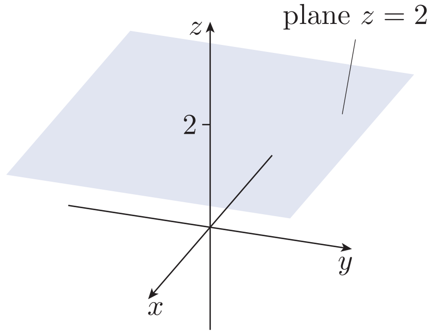
Solution to Exercise A54

Points (x,y,z) that lie in the (y,z)-plane all have $x=0$; so $x=0$ is the equation of this plane.

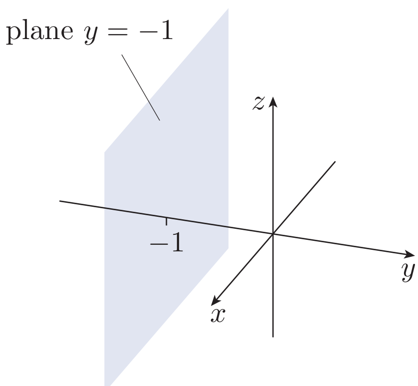
Similarly, points (x,y,z) that lie in the (x,z)-plane all have $y=0$; so $y=0$ is the equation of this plane.

Solution to Exercise A55

(a) This plane is parallel to the (x,y)-plane and passes through the point $(0,0,2)$.



(b) This plane is parallel to the (x,z)-plane and passes through the point $(0,-1,0)$.



Solution to Exercise A56

We use the formula

$$\mathbf{x} \cdot \mathbf{n} = \mathbf{p} \cdot \mathbf{n}$$

for the equation of a plane, where $\mathbf{x} = (x, y, z)$, $\mathbf{n}$ is a normal to the plane and $\mathbf{p}$ is a point in the plane.

(a) Here $\mathbf{n} = (2, 3, 1)$ and $\mathbf{p} = (1, 0, 2)$, so the equation of the plane is

$$(x, y, z) \cdot (2, 3, 1) = (1, 0, 2) \cdot (2, 3, 1).$$

This can be expressed in the form

$$2x + 3y + z = 1 \times 2 + 0 \times 3 + 2 \times 1,$$

that is,

$$2x + 3y + z = 4.$$

(b) Here $\mathbf{n} = (4, -2, 1)$ and $\mathbf{p} = (-1, 1, 5)$, so the equation of the plane is

$$(x, y, z) \cdot (4, -2, 1) = (-1, 1, 5) \cdot (4, -2, 1).$$

This can be expressed in the form

$$4x - 2y + z = (-1) \times 4 + 1 \times (-2) + 5 \times 1,$$

that is,

$$4x - 2y + z = -1.$$

Unit A2
Number systems

Introduction

In this unit you will look at some different systems of numbers, and the rules for combining numbers in these systems. You have met many of these systems before, and you will study some of them in more detail later in the module.

For each number system, you will consider which numbers have additive and/or multiplicative inverses in the system. You will also look at when and how we can solve certain types of equations in the system, such as linear, quadratic and other polynomial equations. The answers to these questions provide insights into the structure of the various number systems, and this in turn enables us to define abstract structures like *fields* and *groups* which share some or all of the properties of number systems and arise in many areas of mathematics. You will meet fields in this unit, and study groups in Books B and E of this module.

1 Real numbers

In this section you will revise real numbers, and some important subsets of the real numbers. You will meet a collection of rules that the arithmetic of real numbers satisfies, and see that some subsets of the real numbers also satisfy these rules, whereas others do not. Finally, you will look at polynomial equations with real coefficients and consider the number of solutions they have.

1.1 Standard subsets of the real numbers

The set of all **real numbers** is denoted by $\mathbb{R}$. This set can be pictured as a number line, often called the **real line**. Each real number is represented by a point on the real line, and each point on this line represents a real number. Thus $\mathbb{R}$ is the set of all numbers that represent lengths along a line (and the negatives of such numbers). For example, the number $\frac{4}{3}$ corresponds to the point that lies a distance $\frac{4}{3}$ from 0 in the positive direction, as shown in Figure 1.

We sometimes refer to real numbers simply as *reals*.

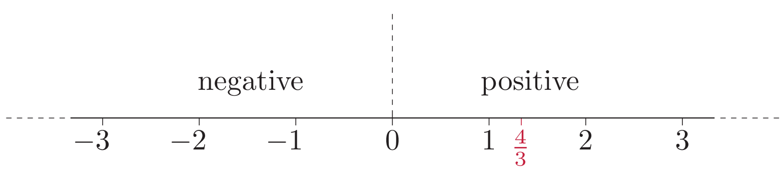


Figure 1 The real line showing the number $\frac{4}{3}$

The following standard subsets of the set $\mathbb{R}$ are used frequently in this module. You met some of them briefly in the previous unit.

The set $\mathbb{R}^*$ is the set of all non-zero real numbers. We can describe this set using set notation in various ways:

$$\begin{aligned}
&\mathbb{R}^* = \mathbb{R} - \{0\},\\
&\mathbb{R}^* = (-\infty, 0) \cup (0, \infty),\\
&\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}.
\end{aligned}$$

The set $\mathbb{Z}$ is the set of **integers**:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

The set $\mathbb{N}$ is the set of positive integers, known as the **natural numbers**:

$$\mathbb{N} = \{n \in \mathbb{Z} : n > 0\} = \{1, 2, 3, \ldots\}.$$

The set $\mathbb{Q}$ is the set of *rational numbers*. A **rational number** is a real number that can be expressed as a fraction whose numerator and denominator are integers. So we can describe $\mathbb{Q}$ using set notation as follows:

$$\mathbb{Q} = \{p/q : p \in \mathbb{Z}, q \in \mathbb{N}\}.$$

Notice that the sets $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$ are related as follows:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}.$$

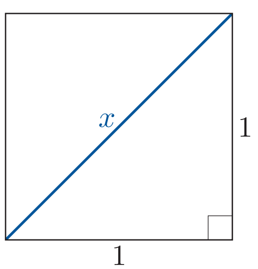
That is, $\mathbb{N}$ is a subset of $\mathbb{Z}$, which in turn is a subset of $\mathbb{Q}$.

Rational numbers and irrational numbers

You have seen that $\mathbb{R}$ is the set of real numbers, and $\mathbb{Q}$ is the set of rational numbers, that is, the set of all numbers that can be expressed as fractions with integer numerators and denominators. The set $\mathbb{Q}$ is certainly a subset of the set $\mathbb{R}$, because each rational number represents a length along the real line (or the negative of such a length), in the way indicated at the beginning of this subsection. But it is not obvious at first sight whether $\mathbb{Q}$ is a *proper* subset of $\mathbb{R}$, or whether $\mathbb{Q}$ and $\mathbb{R}$ are in fact the same set. If it were possible to express every number that represents a length along the real line as a fraction with an integer numerator and denominator, then $\mathbb{Q}$ and $\mathbb{R}$ would be the same set.

In fact, as you will know, they are *not* the same set: some numbers that represent lengths cannot be expressed as fractions with integer numerators and denominators. This is a fact that was discovered by, and was surprising to, the ancient Greeks.

For example, consider the length of the diagonal of a square of side 1, as shown in Figure 2. If this length is x then, by Pythagoras' Theorem, x must satisfy the equation $x^2 = 2$. However, there is no rational number that satisfies this equation.



$x^2 = 1^2 + 1^2 = 2$

Figure 2 The diagonal of a square of side 1

To see this, suppose that there *is* such a number, say $x = p/q$, where p and q are positive integers and p/q is a fraction in lowest terms (so there is no integer greater than 1 that is a factor of both the numerator and denominator). Since $x = p/q$ satisfies the equation $x^2 = 2$, we know that

$$\frac{p^2}{q^2} = 2,$$

which gives $p^2 = 2q^2$, so p^2 is an even number. This tells us that p must also be an even number (because if p were odd, then p^2 would also be odd).

Now, since p is even, we can write $p = 2r$, where r is a positive integer, so $x = 2r/q$. Since x satisfies the equation $x^2 = 2$, we have

$$\frac{4r^2}{q^2} = 2,$$

which gives $q^2 = 2r^2$, so q^2 is an even number. In the same way as for p, this means that q must also be an even number.

But this is impossible: p and q cannot *both* be even, because then 2 would be a factor of both numerator and denominator and p/q is defined as being a fraction in lowest terms. It follows that there is no such rational number p/q. That is, there is no positive rational solution of the equation $x^2 = 2$, and since the negative solution of the equation is obtained simply by changing the sign of the positive solution, we have proved the following theorem.

Theorem A1

There is no rational number x such that $x^2 = 2$.

The proof that you have just seen is a classic example of a *proof by contradiction*. You will learn more about the technique of proof by contradiction, and other useful methods of proof, in the next unit, Unit A3, *Mathematical language and proof*.

So the set $\mathbb{Q}$ is definitely a *proper* subset of $\mathbb{R}$; that is, $\mathbb{R}$ contains numbers that are not in $\mathbb{Q}$. For example, $\mathbb{R}$ contains the number $\sqrt{2}$, which is the positive solution of the equation $x^2 = 2$; thus $\left(\sqrt{2}\right)^2 = 2$. The set $\mathbb{R}$ also contains many other numbers that are not rational numbers, such as $\sqrt{3}$, $\sqrt{7}$ and $\sqrt[3]{2}$ (where $\left(\sqrt[3]{2}\right)^3 = 2$), and so on. Indeed, it can be shown that, if m and n are natural numbers, and the equation $x^m = n$ has no integer solution, then the positive solution of this equation, written as $\sqrt[m]{n}$, cannot be rational.

Other real numbers that are not rational include the number π, which denotes the ratio of the circumference of a circle to its diameter, and the number e, the base for natural logarithms.

The real numbers that are not rational numbers are known as **irrational** numbers.

Johann Lambert

In 1767, in a paper read before the Berlin Academy of Sciences, the Swiss mathematician Johann Heinrich Lambert (1728–1777) provided the first proof that π is irrational. Lambert was a close friend of Leonhard Euler (1707–1783), who had invited him to Berlin in 1764, and of Joseph-Louis Lagrange (1736–1813) who was Euler's successor at the Berlin Academy after Euler returned to St Petersburg in 1766. In addition to this result on π, Lambert is well known for his work in geometry.

We often refer to rational and irrational numbers simply as *rationals* and *irrationals*, respectively.

Decimal expansions of rational numbers and irrational numbers

Every real number has a decimal expansion; for example,

$$\frac{1}{11} = 0.09\,09\,09\,09\ldots,$$
$$1\tfrac{1}{4} = 1.25,$$
$$\pi = 3.141\,592\,653\,589\ldots.$$

The decimal expansion of a *rational* number is always either a **terminating** (that is, finite) decimal, such as 1.25, or a **recurring** decimal, such as $0.09\,09\,09\,09\ldots$, in which the digits repeat in a regular pattern from some position onwards. The decimal representation of any rational number p/q can be obtained by using long division to divide q into p.

On the other hand, the decimal expansion of an *irrational* number is neither finite nor recurring. Instead, it continues for ever, with no pattern of digits that repeats indefinitely, such as π.

Every possible decimal number, finite or infinite, recurring or non-recurring, represents a real number.

1.2 Arithmetic of real numbers

Throughout your previous mathematical studies you will have used various rules of arithmetic whenever you carried out a calculation or an algebraic manipulation. For example, you will be familiar with the rule that the order in which you add or multiply two numbers does not affect the result, and with the rules for multiplying out brackets. Many of these rules of arithmetic come from the eleven simple properties of addition and multiplication of real numbers given in the box below.

Arithmetic in $\mathbb{R}$

Properties for addition

A1 Closure For all $a, b \in \mathbb{R}$,

$$a + b \in \mathbb{R}.$$

A2 Associativity For all $a, b, c \in \mathbb{R}$,

$$a + (b + c) = (a + b) + c.$$

A3 Additive identity For all $a \in \mathbb{R}$,

$$a + 0 = a = 0 + a.$$

A4 Additive inverses For each $a \in \mathbb{R}$, there is a number $-a \in \mathbb{R}$ such that

$$a + (-a) = 0 = (-a) + a.$$

A5 Commutativity For all $a, b \in \mathbb{R}$,

$$a + b = b + a.$$

Properties for multiplication

M1 Closure For all $a, b \in \mathbb{R}$,

$$a \times b \in \mathbb{R}.$$

M2 Associativity For all $a, b, c \in \mathbb{R}$,

$$a \times (b \times c) = (a \times b) \times c.$$

M3 Multiplicative identity For all $a \in \mathbb{R}$,

$$a \times 1 = a = 1 \times a.$$

M4 Multiplicative inverses For each $a \in \mathbb{R}^*$, there is a number $a^{-1} \in \mathbb{R}$ such that

$$a \times a^{-1} = 1 = a^{-1} \times a.$$

M5 Commutativity For all $a, b \in \mathbb{R}$,

$$a \times b = b \times a.$$

Property combining addition and multiplication

D1 Distributivity For all $a, b, c \in \mathbb{R}$,

$$a \times (b + c) = (a \times b) + (a \times c).$$

For clarity, the multiplication properties (M1 to M5) are shown in the above box using the symbol $\times$ but, as you will know, we often prefer to write simply ab for 'a multiplied by b', rather than $a \times b$.

The closure properties (A1 and M1) simply say that adding or multiplying two real numbers results in another real number.

The numbers 0 and 1 are known as the **additive identity** and **multiplicative identity** of $\mathbb{R}$, respectively. The number $-a$ in property A4 is known as the **additive inverse** or **negative** of a. The number a^{-1} in property M4 is known as the **multiplicative inverse** or **reciprocal** of a. One number, namely 0, does not have a multiplicative inverse, since there is no number that multiplies with 0 to make 1, and so 0 is excluded in the multiplicative inverses property (M4).

The set of rational numbers, $\mathbb{Q}$, also satisfies the eleven properties in the box above, in the sense that if $\mathbb{R}$ is replaced by $\mathbb{Q}$ throughout the box, then the properties are still true. (Of course, in property M4 the number 0 is excluded, just as for the real numbers.) You will see later that the same properties hold for the set of complex numbers, $\mathbb{C}$. However, if we restrict ourselves to the set of integers, $\mathbb{Z}$, then one of these properties is no longer true, as you are asked to show in the next exercise.

Exercise A57

(a) Show that $\mathbb{Z}$ does not satisfy the multiplicative inverses property (M4) by giving an example of an integer that does not have a multiplicative inverse.

(b) Which integers have a multiplicative inverse in $\mathbb{Z}$?

A set of numbers, with addition and multiplication defined in such a way that they satisfy the eleven properties in the box, together with a twelfth, rather trivial, property, namely that the additive and multiplicative identities are different numbers, is known as a **field**. (The twelfth property is included for technical reasons to ensure that the set $\{0\}$ with addition and multiplication is not a field; it need not concern you in this module.)

Thus a field is a number system that shares many of the properties of the arithmetic of the real numbers. You have seen that $\mathbb{R}$ and $\mathbb{Q}$ are fields, but that $\mathbb{Z}$ is not a field.

1.3 Solutions of polynomial equations

Even though the sets $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$, with addition and multiplication, are all fields and hence share similar rules of arithmetic, they are quite different in other ways.

Some of their differences are highlighted by considering which polynomial equations, with coefficients in the set in question, have a solution in that set. Here is a reminder of what we mean by a polynomial equation and its coefficients.

Definitions

A **polynomial** in x of **degree** n is an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n$ are numbers, called the **coefficients** of the polynomial, with $a_n \neq 0$.

A **polynomial equation** in x of degree n is an equation of the form $p(x) = 0$, where $p(x)$ is a polynomial in x of degree n.

Polynomial equations (and polynomials) of degrees 1, 2 and 3 are called **linear**, **quadratic** and **cubic**, respectively.

So, for example, the following are polynomials:

$$\tfrac{1}{2}x^3 - x^2 + \sqrt{3}, \quad 2x - 7, \quad x^2 - 2,$$

and the following are polynomial equations:

$$\tfrac{1}{2}x^3 - x^2 + \sqrt{3} = 0, \quad 2x - 7 = 0, \quad x^2 = 2.$$

(The third equation here is a rearrangement of $x^2 - 2 = 0$.)

The equation $x^2 = 2$ is a polynomial equation with coefficients in $\mathbb{Q}$, and you saw earlier in this section that this equation has no solution in $\mathbb{Q}$. However, the equation $x^2 = 2$ can also be considered as an equation with coefficients in $\mathbb{R}$, and it does have solutions in $\mathbb{R}$, namely the two solutions $\pm\sqrt{2}$. In this sense, $\mathbb{R}$ seems a 'better' number system than $\mathbb{Q}$.

In the next exercise, you are asked to look at some *linear* equations, and consider whether they have solutions in the sets $\mathbb{Q}$ and $\mathbb{R}$.

Exercise A58

(a) The following linear equations have coefficients in $\mathbb{Q}$. Determine whether each of them has a solution in $\mathbb{Q}$.

(i) $5x + 10 = 0$ (ii) $5x + 1 = 0$

(b) The following linear equations have coefficients in $\mathbb{R}$. Determine whether each of them has a solution in $\mathbb{R}$.

(i) $2x - 6 = 0$ (ii) $\sqrt{3}x + 7 = 0$

In fact, every linear equation with coefficients in $\mathbb{Q}$ has a solution in $\mathbb{Q}$, because the equation $ax + b = 0$ where $a, b \in \mathbb{Q}$ and $a \neq 0$ has exactly one solution, namely $x = -b/a$, which is rational. (Here we have used properties A2–A4 and M1–M5 to deduce that $x = -ba^{-1} \in \mathbb{Q}$, although we usually express this using 'division' as $x = -b/a \in \mathbb{Q}$.) Similarly, every linear equation with coefficients in $\mathbb{R}$ has exactly one solution in $\mathbb{R}$.

Let us now look at quadratic equations. The example of the quadratic equation $x^2 = 2$ has already shown you that not every quadratic equation with coefficients in $\mathbb{Q}$ has a solution in $\mathbb{Q}$. In the next exercise, you are asked to look at some quadratic equations with coefficients in $\mathbb{R}$, and consider whether they have solutions in $\mathbb{R}$.

Remember that it is usually best to solve a quadratic equation by *factorisation* if you can. Otherwise, you can use the **quadratic formula**, which tells you that the solutions of the quadratic equation $ax^2 + bx + c = 0$, where $a, b, c \in \mathbb{R}$ and $a \neq 0$, are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Exercise A59

Solve the following quadratic equations, stating how many solutions each equation has in $\mathbb{R}$.

(a) $x^2 - 7x + 12 = 0$ (b) $x^2 + 6x + 9 = 0$ (c) $2x^2 + 5x - 3 = 0$

(d) $2x^2 - 2x - 1 = 0$ (e) $x^2 - 2x + 5 = 0$ (f) $x^2 - 2\sqrt{3}x + 3 = 0$

Exercise A59 illustrates that some quadratic equations with coefficients in $\mathbb{R}$ have two solutions in $\mathbb{R}$, some have only one and some have none. In either of the first two cases, the solutions may be rational or irrational. Although you may be accustomed to equations with integer coefficients such as those in Exercise A59(a)–(e), these facts still apply if some or all of the coefficients are irrational; that is, if the coefficients are any real numbers.

So, although the set $\mathbb{R}$ seems 'better' than the set $\mathbb{Q}$, working with $\mathbb{R}$ still does not enable us to find solutions of *all* quadratic equations. In Section 2 you will see that working with the set of complex numbers, $\mathbb{C}$, *does* enable us to find solutions of *all* quadratic equations, and in fact it enables us to find solutions of all polynomial equations.

1.4 The Factor Theorem

In the previous subsection we looked at the issue of whether polynomial equations with coefficients in $\mathbb{Q}$ or in $\mathbb{R}$ have solutions in $\mathbb{Q}$ or in $\mathbb{R}$, respectively. We now confine our attention to polynomial equations with coefficients in $\mathbb{R}$, and consider the maximum number of solutions that such an equation of degree n can have. For example, you already know that a linear equation (that is, a polynomial equation of degree 1) has exactly one solution, and a quadratic equation (that is, a polynomial equation of degree 2) has a maximum of two solutions. We also look at ways in which we can sometimes find some or all of the solutions of a polynomial equation.

We will mainly discuss these issues in terms of polynomials, rather than polynomial equations. We make the following definition.

Definition

The **roots** (or **zeros**) of a polynomial $p(x)$ are the solutions of the equation $p(x) = 0$.

So finding the roots of a polynomial $p(x)$ means the same as finding the solutions of the polynomial equation $p(x) = 0$.

A polynomial with coefficients in $\mathbb{R}$ is called a **real polynomial**.

You know that you can often find the roots of a quadratic polynomial by *factorising* it. Factorisation can also be useful for higher-degree polynomials. In general, if a polynomial $p(x)$ can be expressed in the form

$$p(x) = s(x)t(x),$$

where $s(x)$ and $t(x)$ are polynomials whose degree is less than that of $p(x)$, then we say that $s(x)$ and $t(x)$ are **factors** of $p(x)$.

The following theorem can help us to factorise polynomials. You will see a proof of this theorem in Unit A3.

Theorem A2 Factor Theorem (in $\mathbb{R}$)

Let $p(x)$ be a real polynomial, and let $\alpha \in \mathbb{R}$. Then $p(\alpha) = 0$ if and only if $x - \alpha$ is a factor of $p(x)$.

The phrase 'if and only if' is a means of stating two *converse* mathematical statements at once; here it tells us that the following two statements are both true:

- If $p(\alpha) = 0$, then $x - \alpha$ is a factor of $p(x)$.
- If $x - \alpha$ is a factor of $p(x)$, then $p(\alpha) = 0$.

You will revise the use of the phrase 'if and only if' in more detail in Unit A3.

The following worked exercise demonstrates how you can use the Factor Theorem. It also demonstrates how, once you know that a particular polynomial $p(x)$ has a factorisation of the form $p(x) = (x - \alpha)q(x)$, where you know the value of the root α, you can find the polynomial $q(x)$ by **equating corresponding coefficients**, also known as *comparing coefficients*.

Worked Exercise A24

Show that $x - 2$ is a factor of the cubic polynomial

$$p(x) = x^3 + x^2 - x - 10,$$

and find the corresponding factorisation of $p(x)$.

Solution

Evaluate $p(2)$ and apply the Factor Theorem.

We have

$$p(2) = 2^3 + 2^2 - 2 - 10 = 8 + 4 - 2 - 10 = 0.$$

So, by the Factor Theorem (Theorem A2), $p(x)$ has the factor $x - 2$.

So, since $p(x)$ is a cubic polynomial, it must be the product of $x - 2$ and a quadratic polynomial.

Hence

$$x^3 + x^2 - x - 10 = (x - 2)(ax^2 + bx + c),$$

for some real numbers a, b and c.

To find the coefficients a, b and c of the quadratic polynomial, compare coefficients on each side of the equation. Start with the coefficients of the highest-degree terms and the constant terms.

Equating the coefficients of x^3 gives $1 = a$. Equating the constant terms gives $-10 = -2c$, so $c = 5$. Thus we have

$$x^3 + x^2 - x - 10 = (x - 2)(x^2 + bx + 5).$$

We can compare the coefficients of x^2 or x; we choose x^2.

Equating the coefficients of x^2 gives $1 = -2 + b$, so $b = 3$. Hence

$$x^3 + x^2 - x - 10 = (x - 2)(x^2 + 3x + 5).$$

We can equate the coefficients of x to check our answer. This gives $-1 = 5 - 2b$, so again $b = 3$, as expected.

Exercise A60

(a) For what value of k is $x + 3$ a factor of

$$p(x) = x^3 + kx^2 + 6x + 36\,?$$

(b) For this value of k, find the corresponding factorisation of $p(x)$.

The following theorem can be proved by repeatedly applying the Factor Theorem, as you will see in Unit A3.

Theorem A3

Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a real polynomial, and suppose that $p(x)$ has n distinct real roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n).$$

For example, the polynomial

$$p(x) = 2x^4 - 8x^3 - 2x^2 + 32x - 24$$

has the four distinct real roots 1, 2, 3 and -2, as you can check by evaluating $p(1)$, $p(2)$, $p(3)$ and $p(-2)$, and so (from Theorem A3)

$$p(x) = 2(x - 1)(x - 2)(x - 3)(x + 2).$$

In fact, as you will see in Subsection 2.4, *every* real polynomial $p(x)$ of degree n has a factorisation of the form given in Theorem A3, although the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ need not be distinct and may include non-real *complex numbers*. We have the following.

A real polynomial of degree n has at most n distinct roots (some of which may be complex numbers).

We now look at ways in which you can sometimes find some or all of the roots of a real polynomial.

The following useful observation should be familiar from your previous studies of factorising quadratics. If you multiply out the brackets

$$(x - \alpha)(x - \beta),$$

where α and β are real numbers, then you obtain a quadratic polynomial $p(x) = x^2 + bx + c$ such that

- the value of c, the constant term, is $\alpha\beta$;
- the value of b, the coefficient of x, is $-(\alpha + \beta)$.

We can make a similar observation about the result of multiplying out the n brackets

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

When we multiply out these brackets, we obtain a polynomial of degree n such that the coefficient of x^n is 1. This polynomial has the following properties.

Suppose that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are real numbers. Then

- $a_0 = (-1)^n\alpha_1\alpha_2\cdots\alpha_n$;
- $a_{n-1} = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$.

For example,

$$x^3 + x^2 - 5x + 3 = (x-1)(x-1)(x+3),$$

so $a_0 = 3$, $\alpha_1 = 1$, $\alpha_2 = 1$, $\alpha_3 = -3$ and $a_{n-1} = 1$ and we have

$$3 = (-1)^3 \times 1 \times 1 \times (-3)$$

and

$$1 = -(1 + 1 - 3).$$

The expression for the constant term a_0 in the box above is obtained by comparing constant terms on each side of the equation at the top of the box.

Similarly, the expression for the coefficient a_{n-1} is obtained by equating the corresponding coefficients of x^{n-1}, as follows. When the brackets on the right-hand side are multiplied out, each term in x^{n-1} arises by choosing the variable x from $n-1$ of the brackets, and the constant term from the remaining bracket. Choosing the constant term from the first bracket gives $-\alpha_1x^{n-1}$, choosing the constant term from the second bracket gives $-\alpha_2x^{n-1}$, and so on. Adding all these terms and comparing the resulting total coefficient with the coefficient of x^{n-1} on the left-hand side gives $a_{n-1} = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$.

The observations in the box above can help us factorise a polynomial if we know that all of its roots are integers.

Worked Exercise A25

Given that all the roots of the polynomial

$$p(x) = x^3 - 6x^2 - 9x + 14$$

are integers, write $p(x)$ as a product of linear factors.

Solution

By the first property above, all the roots are factors of 14.

Since all the roots of $p(x)$ are integers, the only possible roots are the factors of 14, that is, ± 1, ± 2, ± 7, ± 14. Considering these in turn, we obtain the following table.

x	1	-1	2	-2	7	-7	14	-14
$p(x)$	0	16	-20	0	0	-560	1456	-3780

The only roots of $p(x)$ are $x = 1$, $x = -2$ and $x = 7$.

Actually, since we know that a cubic polynomial has at most only three roots, we do not need to complete the table once we have found three!

Also, the coefficient of the highest power of x in $p(x)$ is 1. Hence (by Theorem A3)

$$p(x) = (x - 1)(x + 2)(x - 7).$$

As a check, we note that the coefficient of x^2 is equal to minus the sum of the roots, $-6 = -(1 - 2 + 7)$.

Exercise A61

(a) Given that all the roots of the polynomial

$$p(x) = x^3 - 9x^2 + 23x - 15$$

are integers, write $p(x)$ as a product of linear factors.

(b) Given that all the solutions are integers, solve the equation

$$x^3 - 3x^2 + 4 = 0.$$

Use the property relating the sum of the roots to the coefficient of x^2 to write the equation as a product of linear factors.

Exercise A62

(a) Determine a polynomial equation whose solutions are $1, 2, 3, -3$.

(b) Determine a cubic equation whose only solutions are 2 and 3.

2 Complex numbers

In this section you will revise complex numbers and their properties. You will see how to find complex roots of certain polynomial equations, and how the complex exponential function can be used to represent complex numbers.

2.1 What is a complex number?

Earlier you saw that the real numbers correspond to points on the real line. In this subsection you will see that the *complex numbers* correspond to points in the plane.

Complex numbers arise naturally as solutions of quadratic equations. You have seen that some quadratic equations have no solutions in $\mathbb{R}$, that is, no real solutions. For example, you saw in Exercise A59(e) that the equation $x^2 - 2x + 5 = 0$ has no real solutions, because there is no real number whose square is -16. We can extend the set of real numbers to ensure that every quadratic equation has at least one solution.

To do this, we introduce a new number, denoted by i, which is defined to have the property that $i^2 = -1$. We assume that i combines with itself, and with real numbers, according to the usual rules of arithmetic. In particular, we assume that if we multiply i by any real number y then we obtain the product $iy = yi$, and if we then add this product to any real number x we obtain the sum $x + iy = x + yi$. Sums of this form are known as *complex numbers*, and they are the numbers we need to enable us to find solutions of every quadratic equation.

Definitions

A **complex number** is an expression of the form $x + iy$, where x and y are real numbers and $i^2 = -1$. The set of all complex numbers is denoted by $\mathbb{C}$.

A complex number $z = x + iy$ has **real part** x and **imaginary part** y; we write

$$\operatorname{Re} z = x \quad \text{and} \quad \operatorname{Im} z = y.$$

Two complex numbers are equal when their real parts *and* their imaginary parts are equal.

Remarks

1. Any real number x can be written in the form $x + i0$, and any complex number of the form $x + i0$ is usually written simply as x. In this sense, $\mathbb{R}$ is a subset of $\mathbb{C}$. The complex number $0 + i0$ is written as 0.
2. We follow the usual practice of writing a general complex number as $x + iy$, but a particular complex number as, for example, $2 + 3i$, rather than $2 + i3$.

   We also write $2 - 3i$ rather than $2 + (-3)i$, and we write $2 + i\sqrt{3}$ rather than $2 + \sqrt{3}i$, to avoid confusion with $2 + \sqrt{3i}$ (where the number i is included under the square root).
3. Note that $\operatorname{Re} z$ and $\operatorname{Im} z$ are both real numbers. For example, if $z = 2 - 3i$, then $\operatorname{Re} z = 2$ and $\operatorname{Im} z = -3$.
4. A complex number of the form $0 + iy$ (where $y \neq 0$) is sometimes called an **imaginary number**.

You know that every positive real number has two square roots. When you are working with the complex numbers, every negative real number also has two square roots, as follows.

Square roots of a negative real number

For a positive real number d, the square roots of $-d$ are $\pm i\sqrt{d}$.

You can check that $\pm i\sqrt{d}$ are square roots of $-d$ by using the usual rules of arithmetic:

$$\left(\pm i\sqrt{d}\right)^2 = i^2 \left(\sqrt{d}\right)^2 = (-1) \times d = -d.$$

You will see in Subsection 2.4 why these are the *only* square roots of $-d$.

We can solve quadratic equations that have no real solutions by using the fact in the box above, together with the quadratic formula. When we apply this formula to a quadratic equation that has no real solutions, we obtain a term in the numerator of the form $\pm\sqrt{-d}$, where d is a positive number. In real terms, this is meaningless, because the square root sign applies only to positive real numbers, or zero. However, when we are working with complex numbers, we can take this term to mean the two square roots of $-d$, which are as given in the box above. This is illustrated in the worked exercise below.

The equation in this worked exercise is the one from Exercise A59(e), rewritten using z as the variable name. We often use the letter z for a **complex variable** (a variable that represents a complex number).

Worked Exercise A26

Solve the quadratic equation

$$z^2 - 2z + 5 = 0.$$

Solution

The quadratic formula gives

$$z = \frac{2 \pm \sqrt{-16}}{2} = \frac{2 \pm i\sqrt{16}}{2} = \frac{2 \pm 4i}{2} = 1 \pm 2i.$$

We can check that the two complex numbers found in Worked Exercise A26 satisfy the equation we were trying to solve. We use the usual rules of arithmetic, and substitute -1 for i^2 wherever it appears.

For example, if $z = 1 + 2i$, then

$$\begin{aligned} z^2 - 2z + 5 &= (1+2i)^2 - 2(1+2i) + 5 \\ &= 1 + 4i + 4i^2 - 2 - 4i + 5 \\ &= 1 + 4i + 4(-1) - 2 - 4i + 5 \\ &= 1 + 4i - 4 - 2 - 4i + 5 \\ &= 0. \end{aligned}$$

The solution $z = 1 - 2i$ can be checked in the same way.

Similarly, it can be checked that the method of Worked Exercise A26 will in general give us two complex numbers that satisfy the quadratic equation we are trying to solve. So the use of the number i enables us to find solutions of any quadratic equation. You will see later in this section that the use of i ensures that *all* polynomial equations have solutions, even those whose coefficients are themselves complex numbers. This, in turn, means that *any* polynomial can be factorised into a product of linear factors; for example,

$$\begin{aligned} z^2 - 2z + 5 &= (z - (1+2i))(z - (1-2i)) \\ &= (z - 1 - 2i)(z - 1 + 2i). \end{aligned}$$

Exercise A63

Solve the following equations, giving all solutions in $\mathbb{C}$.

(a) $z^2 - 4z + 7 = 0$

(b) $z^2 - iz + 2 = 0$

(c) $z^3 - 3z^2 + 4z - 2 = 0$ (*Hint*: $z = 1$ is one solution.)

(d) $z^4 - 16 = 0$

The complex plane

Just as there is a one-to-one correspondence between the real numbers and the points on the real line, so there is a one-to-one correspondence between the complex numbers and the points in the plane. This correspondence is given by

$$\begin{aligned} f\colon \mathbb{C} &\longrightarrow \mathbb{R}^2 \\ x+iy &\longmapsto (x,y). \end{aligned}$$

Thus we can represent points in the plane by complex numbers and, conversely, we can represent complex numbers by points in the plane. When we do this, we refer to the plane as the **complex plane**, and we often refer to the complex numbers as *points* in the complex plane. A diagram, such as Figure 3, showing complex numbers represented as points in the plane in this way is sometimes called an **Argand diagram**.

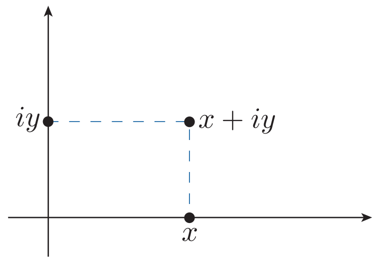


Figure 3 The complex plane

The first widely recognised publication of this idea appeared in a manuscript *Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques* dated 1806 by a mathematician described only as Monsieur Argand. Until recently he was believed to be Jean-Robert Argand but further research by Gert Schubring (2001), first presented in 1998, has shown that this is a misattribution and his first name is unknown.

(Source: Schubring, G. (2001) 'Argand and the early work on graphical representation: New sources and interpretations', *Proceedings of the Wessel Symposium at the Royal Danish Academy of Sciences and Letters*. Copenhagen, August 11–15 1998, pp. 125–146.)

Real numbers are represented in the complex plane by points on the horizontal axis; this axis is called the **real axis**. Similarly, numbers of the form iy are represented by points on the vertical axis; this axis is called the **imaginary axis**.

Exercise A64

Draw a diagram showing each of the following points in the complex plane:

$$2+3i, \quad -3+2i, \quad -2-i, \quad 3-2i.$$

2.2 Arithmetic of complex numbers

Arithmetic operations on complex numbers are carried out as for real numbers, except that we replace i^2 by -1 wherever it occurs.

Worked Exercise A27

Let $z_1 = 1 + 2i$ and $z_2 = 3 - 4i$. Determine the following complex numbers.

(a) $z_1 + z_2$ (b) $z_1 - z_2$ (c) $z_1 z_2$ (d) z_1^2

Solution

The usual rules of arithmetic apply, with the additional property that $i^2 = -1$.

(a) $$\begin{aligned} z_1 + z_2 &= (1 + 2i) + (3 - 4i) \\ &= (1 + 3) + (2 - 4)i \\ &= 4 - 2i \end{aligned}$$

(b) $$\begin{aligned} z_1 - z_2 &= (1 + 2i) - (3 - 4i) \\ &= (1 - 3) + (2 + 4)i \\ &= -2 + 6i \end{aligned}$$

(c) $$\begin{aligned} z_1 z_2 &= (1 + 2i)(3 - 4i) \\ &= 3 + 6i - 4i - 8i^2 \\ &= 3 + 2i + 8 \\ &= 11 + 2i \end{aligned}$$

(d) $$\begin{aligned} z_1^2 &= (1 + 2i)(1 + 2i) \\ &= 1 + 2i + 2i + 4i^2 \\ &= 1 + 4i - 4 \\ &= -3 + 4i \end{aligned}$$

Worked Exercise A27 illustrates how we add, subtract and multiply two given complex numbers. We can apply the same methods to two general complex numbers $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, and obtain the following formal definitions of addition, subtraction and multiplication in $\mathbb{C}$.

Definitions

Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$ be any complex numbers. Then the following operations can be applied.

Addition $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$

Subtraction $z_1 - z_2 = (x_1 - x_2) + i(y_1 - y_2)$

Multiplication $z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_2 y_1 + x_1 y_2)$

There is no need to remember or look up these formulas. For calculations, you can use the methods of Worked Exercise A27. Note that, since the usual rules of algebra hold, so do familiar algebraic identities such as

$$(z_1 + z_2)^2 = z_1^2 + 2z_1z_2 + z_2^2$$

and

$$z_1^2 - z_2^2 = (z_1 - z_2)(z_1 + z_2).$$

An obvious omission from the list of definitions in the box above is *division*. We will return to division after looking at the *complex conjugate* and *modulus* of a complex number.

Exercise A65

Determine the following complex numbers.

(a) $(3 - 5i) + (2 + 4i)$ (b) $(2 - 3i)(-3 + 2i)$ (c) $(5 + 3i)^2$

(d) $(1 + i)(7 + 2i)(4 - i)$

Complex conjugate

Many manipulations involving complex numbers, such as division, can be simplified by using the idea of a *complex conjugate*.

Definition

The **complex conjugate** $\overline{z}$ of the complex number $z = x + iy$ is the complex number $x - iy$.

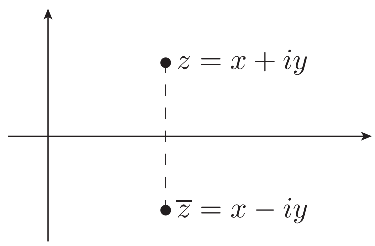


Figure 4 The complex conjugate

For example, if $z = 1 - 2i$, then $\overline{z} = 1 + 2i$. In geometric terms, $\overline{z}$ is the image of z under reflection in the real axis, as shown in Figure 4.

Exercise A66

Let $z_1 = -2 + 3i$ and $z_2 = 3 - i$. Write down $\overline{z_1}$ and $\overline{z_2}$, and draw a diagram showing z_1, z_2, $\overline{z_1}$ and $\overline{z_2}$ in the complex plane.

The following properties of complex conjugates are particularly useful.

Properties of complex conjugates

Let z_1, z_2 and z be any complex numbers. Then:

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
2. $\overline{z_1 z_2} = \overline{z_1} \times \overline{z_2}$
3. $z + \overline{z} = 2\,\mathrm{Re}\,z$
4. $z - \overline{z} = 2i\,\mathrm{Im}\,z$.

To prove that property 1 holds, we consider two arbitrary complex numbers. Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$. Then

$$\begin{aligned}\overline{z_1 + z_2} &= \overline{(x_1 + x_2) + i(y_1 + y_2)}\\ &= (x_1 + x_2) - i(y_1 + y_2)\\ &= (x_1 - iy_1) + (x_2 - iy_2)\\ &= \overline{z_1} + \overline{z_2}.\end{aligned}$$

Exercise A67

Use a similar approach to prove that properties 2, 3 and 4 all hold.

Modulus of a complex number

We also need the idea of the *modulus* of a complex number. Recall that the modulus of a real number x is defined by

$$|x| = \begin{cases} x, & \text{if } x \geq 0,\\ -x, & \text{if } x < 0.\end{cases}$$

For example, $|7| = 7$ and $|-6| = 6$.

In other words, $|x|$ is the distance from the point x on the real line to the origin. We extend this definition to complex numbers, as illustrated in Figure 5.

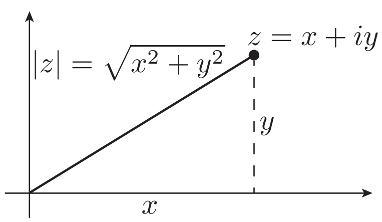


Figure 5 The modulus of a complex number

Definition

The **modulus** $|z|$ of a complex number z is the distance from the point z in the complex plane to the origin.

Thus the modulus of the complex number $z = x + iy$ is

$$|z| = \sqrt{x^2 + y^2}.$$

For example, if $z = 3 - 4i$, then $|z| = \sqrt{3^2 + (-4)^2} = \sqrt{25} = 5$.

Exercise A68

Determine the modulus of each of the following complex numbers.

(a) $5+12i$ (b) $1+i$ (c) -5

The modulus of a complex number has many properties similar to those of the modulus of a real number.

Properties of the modulus

1. $|z| \geq 0$ for any $z \in \mathbb{C}$, with equality only when $z = 0$.
2. $|z_1 z_2| = |z_1|\,|z_2|$ for any $z_1, z_2 \in \mathbb{C}$.

Property 1 is clear from the definition of $|z|$. Property 2 can be shown to hold in a similar way to property 2 of complex conjugates in the solution to Exercise A67.

The following useful result shows the link between modulus and distance in the complex plane.

Distance formula for $\mathbb{C}$

The distance between the points z_1 and z_2 in the complex plane is $|z_1 - z_2|$.

This is obtained by applying Pythagoras' Theorem to the triangle shown in Figure 6. The formula holds wherever the points z_1 and z_2 are situated in the complex plane.

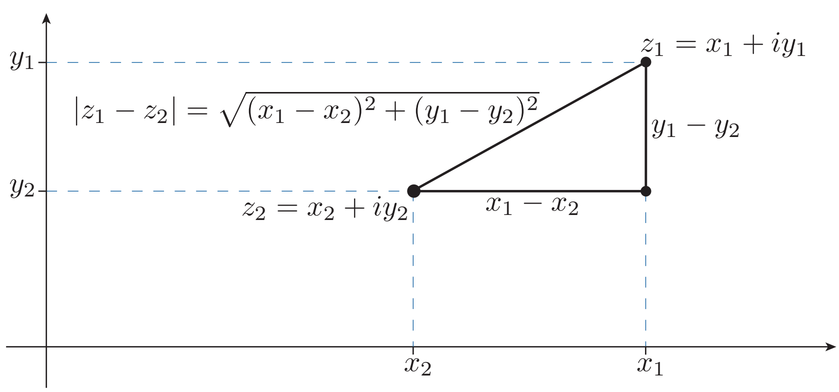


Figure 6 The distance formula for $\mathbb{C}$

Exercise A69

For each of the following pairs z_1, z_2 of complex numbers, draw a diagram showing z_1 and z_2 in the complex plane, find $z_1 - z_2$ and evaluate $|z_1 - z_2|$.

(a) $z_1 = 3 + i, \quad z_2 = 1 + 2i.$

(b) $z_1 = 1, \quad z_2 = i.$

(c) $z_1 = -5 - 3i, \quad z_2 = 2 - 7i.$

The following properties describe the relationship between the modulus and the complex conjugate of a complex number.

Conjugate–modulus properties

1. $|\overline{z}| = |z|$ for all $z \in \mathbb{C}$.
2. $z\overline{z} = |z|^2$ for all $z \in \mathbb{C}$.

To see why these properties hold, let $z = x + iy$. Then $\overline{z} = x - iy = x + i(-y)$, so

$$|\overline{z}| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|.$$

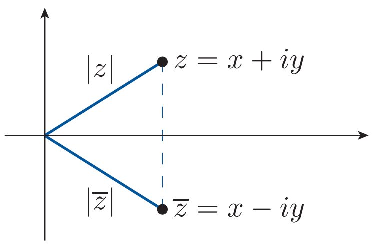


Figure 7 The complex conjugate

This can also be seen geometrically in Figure 7, where the distances from the origin to both z and its complex conjugate $\overline{z}$ are the same. We also have

$$z\overline{z} = (x + iy)(x - iy) = x^2 + ixy - ixy - i^2y^2 = x^2 + y^2 = |z|^2.$$

Division of complex numbers

The second of the conjugate–modulus properties in the above box enables us to find reciprocals of complex numbers and to divide one complex number by another, as shown in the next worked exercise. In exactly the same way as for real numbers, we cannot find a reciprocal of zero, nor divide any complex number by zero.

Worked Exercise A28

(a) Find the reciprocal of $2 - 5i$.

(b) Find the quotient $\dfrac{3 - i}{1 + 2i}$.

Solution

(a) To express the reciprocal $1/(2-5i)$ in the form $a+ib$, we multiply the numerator and denominator by $2+5i$, the complex conjugate of the denominator $2-5i$, and then use the second conjugate–modulus property.

The reciprocal is

$$\begin{aligned}\frac{1}{2-5i} &= \frac{1(2+5i)}{(2-5i)(2+5i)} \\ &= \frac{2+5i}{|2-5i|^2} \\ &= \frac{2+5i}{4+25} \\ &= \tfrac{2}{29} + \tfrac{5}{29}i = \tfrac{1}{29}(2+5i).\end{aligned}$$

(b) We multiply the numerator and denominator by $1-2i$, the complex conjugate of the denominator $1+2i$, and then use the second conjugate–modulus property.

$$\begin{aligned}\frac{3-i}{1+2i} &= \frac{(3-i)(1-2i)}{(1+2i)(1-2i)} \\ &= \frac{3-i-6i+2i^2}{|1+2i|^2} \\ &= \frac{1-7i}{1+4} \\ &= \tfrac{1}{5} - \tfrac{7}{5}i = \tfrac{1}{5}(1-7i).\end{aligned}$$

The method used in Worked Exercise A28, of multiplying the numerator and denominator by the complex conjugate of the denominator, enables us to find the reciprocal of any non-zero complex number z, and the quotient z_1/z_2 of any two complex numbers z_1 and z_2, where $z_2 \neq 0$. We can obtain general formulas as follows.

For the reciprocal, we have

$$\frac{1}{z} = \frac{1 \times \overline{z}}{z \times \overline{z}} = \frac{\overline{z}}{|z|^2}, \quad \text{for } z \neq 0.$$

If $z = x + iy$, then $\overline{z} = x - iy$ and $|z|^2 = x^2 + y^2$, so we obtain

$$\frac{1}{x+iy} = \frac{x-iy}{x^2+y^2}.$$

For the quotient z_1/z_2, we have

$$\frac{z_1}{z_2} = \frac{z_1 \times \overline{z_2}}{z_2 \times \overline{z_2}} = \frac{z_1\overline{z_2}}{|z_2|^2}, \quad \text{for } z_2 \neq 0.$$

If $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, this can be rewritten as

$$\frac{x_1 + iy_1}{x_2 + iy_2} = \frac{(x_1 + iy_1)(x_2 - iy_2)}{x_2^2 + y_2^2} = \frac{(x_1x_2 + y_1y_2) + i(x_2y_1 - x_1y_2)}{x_2^2 + y_2^2}.$$

These formulas may be used in theoretical work, but for calculations of reciprocals and quotients it is simpler to use the method of Worked Exercise A28.

Exercise A70

Find the reciprocal of each of the following complex numbers.

(a) $3 - i$ (b) $-1 + 2i$

Exercise A71

Evaluate each of the following quotients.

(a) $\dfrac{5}{2 - i}$ (b) $\dfrac{2 + 3i}{-3 + 4i}$

Arithmetic properties of complex numbers

The set of complex numbers $\mathbb{C}$ satisfies the eleven properties previously given for arithmetic in $\mathbb{R}$. These properties are stated in the box below (their proofs are not given here). Since $\mathbb{C}$ satisfies these eleven properties (and also satisfies the twelfth, trivial, property mentioned in Subsection 1.2), it is a *field*, like $\mathbb{R}$ and $\mathbb{Q}$.

Arithmetic in $\mathbb{C}$

Properties for addition

A1 Closure For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 + z_2 \in \mathbb{C}.$$

A2 Associativity For all $z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3.$$

A3 Additive identity For all $z \in \mathbb{C}$,

$$z + 0 = z = 0 + z.$$

A4 Additive inverses For each $z \in \mathbb{C}$, there is a number $-z \in \mathbb{C}$ such that

$$z + (-z) = 0 = (-z) + z.$$

A5 Commutativity For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 + z_2 = z_2 + z_1.$$

Properties for multiplication

M1 Closure For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 \times z_2 \in \mathbb{C}.$$

M2 Associativity For all $z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 \times (z_2 \times z_3) = (z_1 \times z_2) \times z_3.$$

M3 Multiplicative identity For all $z \in \mathbb{C}$,

$$z \times 1 = z = 1 \times z.$$

M4 Multiplicative inverses For each $z \in \mathbb{C} - \{0\}$, there is a number $z^{-1} \in \mathbb{C}$ such that

$$z \times z^{-1} = 1 = z^{-1} \times z.$$

M5 Commutativity For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 \times z_2 = z_2 \times z_1.$$

Property combining addition and multiplication

D1 Distributivity For all $z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 \times (z_2 + z_3) = (z_1 \times z_2) + (z_1 \times z_3).$$

In particular, $0 = 0 + 0i$ plays the same role in $\mathbb{C}$ as the real number 0 does in $\mathbb{R}$: it is the **additive identity**. The number $1 = 1 + 0i$ plays the same role as 1: it is the **multiplicative identity**. We also have that the **additive inverse** (or negative) of $z = x + iy$ is $-z = -x - iy$, and the **multiplicative inverse** (or reciprocal) of $z = x + iy$ is

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2}, \quad \text{for } z \neq 0.$$

However, one very important difference between the set of real numbers and the set of complex numbers is that, unlike the real numbers, the complex numbers are not *ordered*.

Recall that, for any two real numbers a and b, exactly one of the three properties

$$a < b, \quad a = b, \quad \text{or} \quad a > b$$

is true; this is what we mean by saying that the real numbers are ordered. But this is not the case for the complex numbers. For example, given the complex numbers $1 + 2i$ and $-1 + 3i$, we cannot say that one of the following properties is true:

$$1 + 2i > -1 + 3i \quad \text{or} \quad 1 + 2i = -1 + 3i \quad \text{or} \quad 1 + 2i < -1 + 3i.$$

Indeed, inequalities involving complex numbers make sense only if they are inequalities between *real* quantities, such as the moduli of the complex numbers. (Note that 'moduli' is the plural of 'modulus'.) For example, inequalities such as

$$|z - 2i| \leq 3 \quad \text{or} \quad \operatorname{Re} z > 5$$

are valid.

2.3 Polar form

You have seen that the complex number $x + iy$ corresponds to the point (x, y) in the complex plane. This correspondence enables us to give an alternative description of complex numbers, using so-called *polar form*. This form is particularly useful when we discuss properties related to multiplication and division of complex numbers.

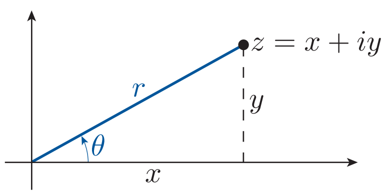


Figure 8 A complex number determined by its modulus and angle

Polar form is obtained by noting that the point in the complex plane associated with the non-zero complex number $z = x + iy$ is uniquely determined by the modulus $r = |z| = \sqrt{x^2 + y^2}$, together with the angle θ (measured in an anticlockwise direction in radians) between the positive direction of the real axis and the line from the origin to the point, as shown in Figure 8. We have

$$x = r\cos\theta \quad \text{and} \quad y = r\sin\theta,$$

so the complex number z can be expressed as

$$z = x + iy = r(\cos\theta + i\sin\theta).$$

This description of z in terms of r and θ is not unique because the angles $\theta \pm 2\pi$, $\theta \pm 4\pi$, $\theta \pm 6\pi$, $\dots$, also determine the same complex number. However, if we restrict the angle θ to lie in the interval $(-\pi, \pi]$, then the description *is* unique. (Some texts restrict θ to lie in the interval $[0, 2\pi)$.)

Note that for the complex number 0, which is represented in the complex plane by the origin, the value of r is 0, and θ is not defined.

Definitions

A non-zero complex number $z = x + iy$ is in **polar form** if it is expressed as

$$z = r(\cos\theta + i\sin\theta),$$

where $r = |z|$ and θ is any angle (measured in radians anticlockwise) between the positive direction of the x-axis and the line joining z to the origin.

Such an angle θ is called an **argument** of the complex number z, and is denoted by $\arg z$. The **principal argument** of z is the value of $\arg z$ that lies in the interval $(-\pi, \pi]$, and is denoted by $\operatorname{Arg} z$.

The term *principal argument* is a shortened form of the more conventional 'principal *value of the* argument'. Some texts use $r\operatorname{cis}\theta$, $r\angle\theta$ or $\langle r,\theta\rangle$ as shorthand for $r(\cos\theta + i\sin\theta)$.

Sometimes we refer to $z = x + iy$ as the **Cartesian form** of z, to distinguish it from the polar form.

We now look at how to convert a complex number from polar form to Cartesian form, and vice versa.

When carrying out such conversions, it is useful to remember the values in the table below, as these will help you in some special cases. You may find it easier to remember the triangles in Figure 9, from which you can work out most of the values in the table.

Sines and cosines of special angles

θ	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
$\sin\theta$	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1
$\cos\theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	0

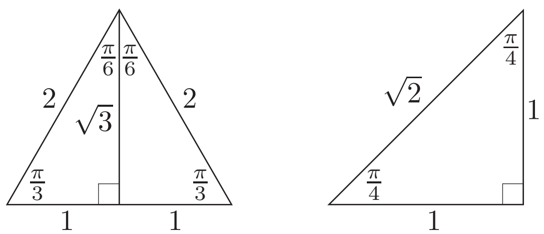


Figure 9 Triangles for finding sines and cosines of special angles

The following trigonometric identities are also helpful; they are included in the module Handbook.

Useful trigonometric identities

For any $\theta \in \mathbb{R}$,

$$\sin(\pi - \theta) = \sin\theta, \qquad \sin(-\theta) = -\sin\theta,$$
$$\cos(\pi - \theta) = -\cos\theta, \qquad \cos(-\theta) = \cos\theta.$$

You may be able to remember these identities by roughly sketching graphs of the sine and cosine functions, and using their symmetry. For example, we can sketch the sine function as in Figure 10.

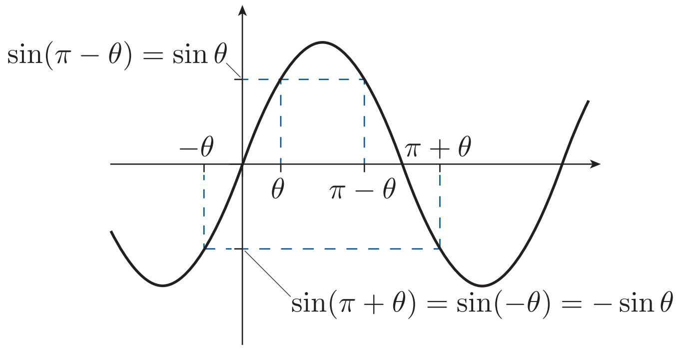


Figure 10 A sketch of the sine function for working out symmetry identities

Converting a complex number from polar form to Cartesian form is straightforward: we simply use the equations

$$x = r\cos\theta, \quad y = r\sin\theta$$

as above to find x and y given r and θ. This is demonstrated in the following worked exercise.

Worked Exercise A29

Express each of the following complex numbers in Cartesian form.

(a) $3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)$ (b) $\cos\left(-\frac{\pi}{6}\right) + i\sin\left(-\frac{\pi}{6}\right)$

Solution

(a) Here $r = 3$ and $\theta = \pi/3$. Thus the required form is $x + iy$, where

$$x = 3\cos\frac{\pi}{3} = 3 \times \tfrac{1}{2} = \tfrac{3}{2}$$

and

$$y = 3\sin\frac{\pi}{3} = 3 \times \frac{\sqrt{3}}{2} = \frac{3\sqrt{3}}{2}.$$

The Cartesian form is therefore $\frac{3}{2}(1 + i\sqrt{3})$.

(b) Here $r = 1$ and $\theta = -\pi/6$. Thus the required form is $x + iy$, where

$$x = \cos\left(-\frac{\pi}{6}\right) = \cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$$

and

$$y = \sin\left(-\frac{\pi}{6}\right) = -\sin\frac{\pi}{6} = -\tfrac{1}{2}.$$

The Cartesian form is therefore $\frac{1}{2}(\sqrt{3} - i)$.

Exercise A72

Express each of the following complex numbers in Cartesian form.

(a) $2\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)$ (b) $4\left(\cos\left(-\frac{2\pi}{3}\right) + i\sin\left(-\frac{2\pi}{3}\right)\right)$

To convert a non-zero complex number z from Cartesian form $x + iy$ to polar form $r(\cos\theta + i\sin\theta)$, we first find the modulus r using the formula

$$r = \sqrt{x^2 + y^2}.$$

Then we find the principal argument θ; recall that this is the angle in the interval $(-\pi, \pi]$ measured in an anticlockwise direction (in radians) between the positive direction of the real axis and the line from the origin to z.

If z is either real or imaginary, then it lies on one of the axes and has principal argument 0, $\pi/2$, π or $-\pi/2$, as shown in Figure 11.

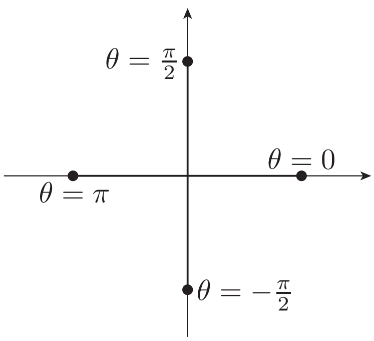


Figure 11 The principal argument θ when z is real or imaginary

Otherwise, to find the principal argument θ we need to solve the equations

$$\cos\theta = \frac{x}{r} \quad \text{and} \quad \sin\theta = \frac{y}{r}, \quad \text{where } \theta \in (-\pi, \pi].$$

We can do this by first finding the acute angle ϕ that satisfies the related equation

$$\cos\phi = \frac{|x|}{r} \quad \left(\text{or, equivalently, } \sin\phi = \frac{|y|}{r} \text{ or } \tan\phi = \left|\frac{y}{x}\right|\right).$$

This acute angle ϕ is the angle at the origin in the right-angled triangle formed by drawing the perpendicular from z to the real axis, as illustrated in Figure 12 in the case where z lies in the second quadrant. (Remember that the quadrants are numbered as shown in Figure 13.)

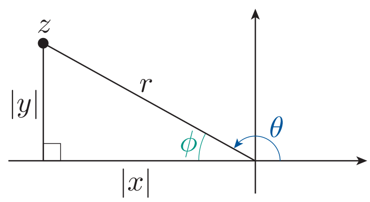


Figure 12 The angles ϕ and θ

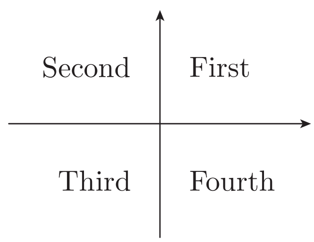


Figure 13 The quadrants of the plane

Once we have found this acute angle ϕ, we can find the principal argument θ by sketching z in the complex plane (the important thing is to get it in the correct quadrant), marking the acute angle ϕ on the sketch, and deducing the principal argument θ. For example, if z is in the third quadrant and $\phi = \pi/3$, then we can see from the sketch in Figure 14 that

$$\theta = -\left(\pi - \frac{\pi}{3}\right) = -\frac{2\pi}{3}.$$

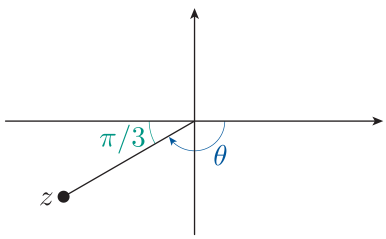


Figure 14 A complex number z in the third quadrant, with $\phi = \pi/3$

In fact, the relationship between the principal argument θ and the acute angle ϕ, for each of the four quadrants in which z can lie, is as shown in Figure 15. So, if you prefer, you can use the appropriate formula from Figure 15 to deduce θ from ϕ. You can also find the quadrant in which z lies by using the values of x and y, without having to sketch z in the complex plane.

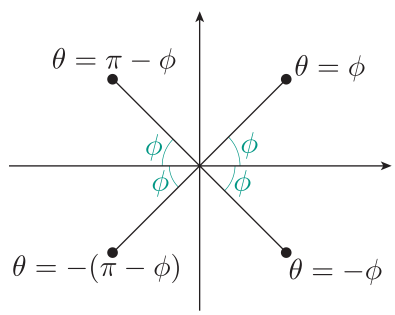


Figure 15 The relationship between θ and ϕ for each quadrant

Both methods for finding θ are illustrated in the next worked exercise.

Worked Exercise A30

Express each of the following complex numbers in polar form, using the principal argument.

(a) $2 + 2i$ (b) $-\frac{1}{2}(1 + i\sqrt{3})$

Solution

(a) Let $z = x + iy = 2 + 2i$, so $x = 2$ and $y = 2$.

Both x and y are positive, so z lies in the first quadrant.

Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{x^2 + y^2} = \sqrt{2^2 + 2^2} = \sqrt{8} = 2\sqrt{2}.$$

To find θ, we calculate

$$\cos\phi = \frac{|x|}{r} = \frac{2}{2\sqrt{2}} = \frac{1}{\sqrt{2}}.$$

So $\phi = \pi/4$, and z lies in the first quadrant so $\theta = \phi = \pi/4$.

The polar form of $2+2i$ in terms of the principal argument is therefore

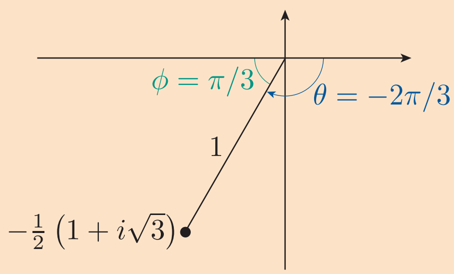
$$2\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right).$$

(b) Let $z=x+iy=-\frac{1}{2}(1+i\sqrt{3})$, so $x=-\frac{1}{2}$ and $y=-\sqrt{3}/2$.

Then $z=r(\cos\theta+i\sin\theta)$, where

$$r=\sqrt{x^2+y^2}=\sqrt{\left(-\frac{1}{2}\right)^2+\left(-\frac{\sqrt{3}}{2}\right)^2}=1.$$

A sketch helps here. We have added on the values for ϕ and θ although they are not known when this is first sketched.



To find θ, we calculate

$$\cos\phi=\frac{|x|}{r}=\frac{|-\frac{1}{2}|}{1}=\tfrac{1}{2}.$$

So $\phi=\pi/3$, and from the drawing we see that $\theta=-(\pi-\phi)=-2\pi/3$.

The polar form of $-\frac{1}{2}(1+i\sqrt{3})$ in terms of the principal argument is therefore

$$\cos\left(-\frac{2\pi}{3}\right)+i\sin\left(-\frac{2\pi}{3}\right).$$

Exercise A73

For each of the following complex numbers, draw a diagram showing its location in the complex plane. Express the complex number in polar form using the principal argument, and mark this argument and the modulus on your diagram.

(a) $-1+i$ (b) $1-i\sqrt{3}$ (c) -5

The following pair of trigonometric identities simplify multiplication of complex numbers in polar form; they are included in the module Handbook.

More useful trigonometric identities

For any $\theta_1, \theta_2 \in \mathbb{R}$,

$$\sin(\theta_1+\theta_2) = \sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2,$$
$$\cos(\theta_1+\theta_2) = \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2.$$

Let

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1) \quad \text{and} \quad z_2 = r_2(\cos\theta_2 + i\sin\theta_2).$$

Then, by the trigonometric identities above,

$$\begin{aligned} z_1z_2 &= r_1(\cos\theta_1 + i\sin\theta_1) \times r_2(\cos\theta_2 + i\sin\theta_2) \\ &= r_1r_2(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2) \\ &= r_1r_2(\cos\theta_1\cos\theta_2 + i\sin\theta_1\cos\theta_2 + i\cos\theta_1\sin\theta_2 + i^2\sin\theta_1\sin\theta_2) \\ &= r_1r_2((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)) \\ &= r_1r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \end{aligned}$$

That is, to multiply two complex numbers in polar form, we *multiply* their moduli and *add* their arguments:

$$z_1z_2 = r_1r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \tag{1}$$

Worked Exercise A31

Find the product z_1z_2 in polar form using the principal argument for the following complex numbers z_1 and z_2:

$$z_1 = 2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \quad \text{and} \quad z_2 = 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right).$$

Solution

$$\begin{aligned} &2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \times 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) \\ &\qquad = 2\times 3\left(\cos\left(\frac{\pi}{4}+\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{4}+\frac{\pi}{3}\right)\right) \\ &\qquad = 6\left(\cos\frac{7\pi}{12} + i\sin\frac{7\pi}{12}\right). \end{aligned}$$

The principal argument lies in the interval $(-\pi, \pi]$.

Since $-\pi < 7\pi/12 \le \pi$, the above expression gives the product z_1z_2 in polar form using the principal argument.

We can also use formula (1) for the product of two complex numbers in polar form to establish a similar formula for the *quotient* of two complex numbers. Specifically, we show that if

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1) \quad \text{and} \quad z_2 = r_2(\cos\theta_2 + i\sin\theta_2),$$

with $z_2 \neq 0$, which implies that $r_2 \neq 0$, then z_1/z_2 is the complex number

$$z = r(\cos\theta + i\sin\theta), \text{ where } r = r_1/r_2 \text{ and } \theta = \theta_1 - \theta_2.$$

To see this, notice that since $r_1 = rr_2$ and $\theta_1 = \theta + \theta_2$ it follows from the discussion above that $z_1 = zz_2$. Hence $z_1/z_2 = z$, as required.

That is, to divide a complex number z_1 by another complex number z_2, we divide the modulus of z_1 by the modulus of z_2, and subtract the argument of z_2 from the argument of z_1:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\theta_1 - \theta_2) + i\sin(\theta_1 - \theta_2)), \text{ where } z_2 \neq 0. \tag{2}$$

Worked Exercise A32

Find the quotient z_1/z_2 in polar form using the principal argument for the following complex numbers z_1 and z_2:

$$z_1 = 2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \quad \text{and} \quad z_2 = 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right).$$

Solution

$$\begin{aligned}\frac{2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)}{3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)} &= \frac{2}{3}\left(\cos\left(\frac{\pi}{4} - \frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{4} - \frac{\pi}{3}\right)\right)\\ &= \frac{2}{3}\left(\cos\left(-\frac{\pi}{12}\right) + i\sin\left(-\frac{\pi}{12}\right)\right).\end{aligned}$$

The principal argument lies in the interval $(-\pi, \pi]$.

Since $-\pi < -\pi/12 \leq \pi$, the above expression gives the quotient z_1/z_2 in polar form using the principal argument.

In particular, if $z = r(\cos\theta + i\sin\theta)$ with $r \neq 0$, then the reciprocal of z is

$$\begin{aligned}\frac{1}{z} &= \frac{1}{r}(\cos(0 - \theta) + i\sin(0 - \theta))\\ &= \frac{1}{r}(\cos(-\theta) + i\sin(-\theta))\\ &= \frac{1}{r}(\cos\theta - i\sin\theta),\end{aligned}$$

so we have the identity

$$\frac{1}{z} = \frac{1}{r}(\cos(-\theta) + i\sin(-\theta)). \tag{3}$$

The methods that you have seen for multiplying complex numbers in polar form can be generalised to apply to a product of several complex numbers. These methods are as summarised in the box below.

Product and quotient in polar form

- To multiply two (or more) complex numbers given in polar form, multiply their moduli and add their arguments.
- To divide a complex number z_1 by a non-zero complex number z_2 when both are given in polar form, divide the modulus of z_1 by the modulus of z_2, and subtract the argument of z_2 from the argument of z_1.

If you want the *principal* argument of a product or quotient, then you may need to add or subtract integer multiples of 2π from the argument calculated, to obtain an angle in the interval $(-\pi, \pi]$.

Exercise A74

Determine the product $z_1 z_2$ and the quotient z_1/z_2 in polar form using the principal argument for the following complex numbers.

(a) $z_1 = 4\left(\cos\left(-\frac{\pi}{6}\right) + i\sin\left(-\frac{\pi}{6}\right)\right)$ and $z_2 = \frac{1}{2}\left(\cos\frac{7\pi}{8} + i\sin\frac{7\pi}{8}\right)$.

(b) $z_1 = 3\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$ and $z_2 = \frac{1}{2}\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)$.

Exercise A75

Let $z_1 = -1 + i$, $z_2 = 1 - i\sqrt{3}$ and $z_3 = -5$.

Express $z_1 z_2 z_3$ and $\dfrac{z_2 z_3}{z_1}$ in polar form using the principal argument.

(You found in Exercise A73 that $-1 + i = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)$,
$1 - i\sqrt{3} = 2\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right)$, and $-5 = 5(\cos\pi + i\sin\pi)$.)

2.4 Complex roots of polynomials

We begin this section with a reminder of what we mean by the word 'root'. In this unit, we use this term in two different, but related, senses, as given below. You met the first of these in Subsection 1.4.

Definitions

If $p(z)$ is a polynomial, then the solutions of the polynomial equation $p(z) = 0$ are called the **roots** of $p(z)$.

If a is a complex number, then the solutions of the equation $z^n = a$ are called the nth **roots** of a.

The two uses of the word 'root' are related as follows: the nth roots of a are the roots of the polynomial $z^n - a$.

Recall that the roots of a polynomial are also called its **zeros**.

In this subsection we look at how to find the nth roots of any complex number, and we consider the roots of polynomial equations more generally.

We can obtain a useful result by considering what happens when we multiply together n copies of the same complex number in polar form. If $z = r(\cos\theta + i\sin\theta)$, then by the method that you saw above for multiplying complex numbers in polar form, we obtain

$$(r(\cos\theta + i\sin\theta))^n = r^n(\cos n\theta + i\sin n\theta), \quad \text{for } n \geq 1. \tag{4}$$

As before, the argument $n\theta$ may not be the *principal* argument of $(\cos\theta + i\sin\theta)^n$, so we may need to add or subtract integer multiples of 2π to obtain an angle in the interval $(-\pi, \pi]$. This is illustrated in the next worked exercise.

Worked Exercise A33

Find z^4, where $z = -1 + i$.

Solution

Find the polar form of z, then apply equation (4).

From Exercise A73(a), we have

$$-1 + i = \sqrt{2}\left(\cos\left(\frac{3\pi}{4}\right) + i\sin\left(\frac{3\pi}{4}\right)\right),$$

so

$$\begin{aligned}(-1+i)^4 &= (\sqrt{2})^4\left(\cos\left(4 \times \frac{3\pi}{4}\right) + i\sin\left(4 \times \frac{3\pi}{4}\right)\right)\\ &= 4(\cos 3\pi + i\sin 3\pi)\end{aligned}$$

We need the principal argument, so subtract 2π to get a value in $(-\pi, \pi]$.

$$= 4(\cos\pi + i\sin\pi) = -4.$$

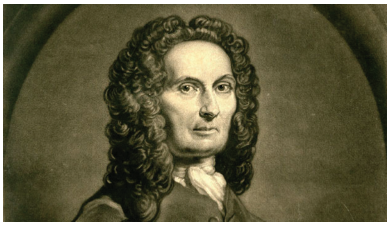
Therefore $z^4 = -4$.

You have seen that equation (4) holds for all $n \geq 1$; in fact, it is true for all integers. This follows from a result known as *de Moivre's Theorem*.

Theorem A4 de Moivre's Theorem

If $z = \cos\theta + i\sin\theta$, then for any $n \in \mathbb{Z}$,

$$z^n = (\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$



Abraham de Moivre

Abraham de Moivre (1667–1754) was a French mathematician who worked in England. He was part of the Huguenot flight from France after the revocation of the Edict of Nantes in 1685 and is first recorded as being in England in late 1686. De Moivre's most important work is *The Doctrine of Chances* (1718), the first textbook for the calculus of probabilities.

To see that de Moivre's Theorem is true for all integers, we need to also consider the cases where $n = 0$ and n is negative. We look at these cases separately, as follows.

For $n = 0$, we have

$$(\cos\theta + i\sin\theta)^0 = 1,$$

and

$$\begin{aligned} \cos(0\times\theta) + i\sin(0\times\theta) &= \cos 0 + i\sin 0 \\ &= 1. \end{aligned}$$

Thus the result holds for $n = 0$.

For $n = -m$, where m is a positive integer, we have

$$\begin{aligned} (\cos\theta + i\sin\theta)^n &= (\cos\theta + i\sin\theta)^{-m} \\ &= \frac{1}{(\cos\theta + i\sin\theta)^m}, \end{aligned}$$

and we know that $(\cos\theta + i\sin\theta)^m = \cos(m\theta) + i\sin(m\theta)$, since m is a positive integer. Therefore

$$\begin{aligned} (\cos\theta + i\sin\theta)^n &= \frac{1}{\cos(m\theta) + i\sin(m\theta)} \\ &= \cos(-m\theta) + i\sin(-m\theta) \quad \text{(by formula (3))} \\ &= \cos n\theta + i\sin n\theta, \end{aligned}$$

as required.

One application of de Moivre's Theorem is in finding the nth roots of complex numbers; that is, in solving equations of the form $z^n = a$, where $a \in \mathbb{C}$. Before you see how to do this, you are asked in the next exercise to use the theorem to verify some solutions of such an equation.

Exercise A76

(a) Write down the complex number 1 in polar form.

(b) Use de Moivre's Theorem to show that each of the three complex numbers with polar forms

$$\cos 0 + i\sin 0, \quad \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} \quad \text{and} \quad \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$$

satisfies the equation $z^3 = 1$.

(c) Write down the three solutions to the equation $z^3 = 1$ given in part (b) in Cartesian form.

The solution to Exercise A76 verifies that the three given complex numbers are solutions of the equation $z^3 = 1$. However, what we really want is a method that will enable us to find solutions of such an equation. Fortunately, de Moivre's Theorem enables us to do this. The method is demonstrated in the next worked exercise.

Worked Exercise A34

Solve the equation $z^3 = -27$. Find the Cartesian form of each solution, and sketch the solutions in the complex plane.

Solution

Write the variable z in polar form, in terms of a variable modulus r and a variable argument θ. Also write the number on the right-hand side of the equation in polar form.

Let $z = r(\cos\theta + i\sin\theta)$. Also, $-27 = 27(\cos\pi + i\sin\pi)$. So the equation $z^3 = 27$ is

$$r^3(\cos\theta + i\sin\theta)^3 = 27(\cos\pi + i\sin\pi).$$

Use de Moivre's Theorem to find the polar form of the left-hand side.

By de Moivre's Theorem, the equation can be written as

$$r^3(\cos 3\theta + i\sin 3\theta) = 27(\cos\pi + i\sin\pi).$$

Find r by comparing moduli on each side.

Comparing moduli gives $r^3 = 27$, so $r = 3$.

Now find θ by comparing arguments on each side. One solution for θ is obtained by taking $3\theta = \pi$. However, we could also take $3\pi,\ 5\pi,\ 7\pi,\ \ldots$ as arguments of -27, so $3\theta = 3\pi$, $3\theta = 5\pi$, $3\theta = 7\pi$, $\ldots$ also give solutions. In general, for any $k \in \mathbb{Z}$, the equation $3\theta = \pi + 2k\pi$, that is, $\theta = \dfrac{\pi}{3} + \dfrac{2k\pi}{3}$, gives a solution. However, as discussed after this worked example, we need consider only $k = 0, 1, 2$, as other values of k just repeat the same three solutions.

The possible values of θ are given by

$$\theta = \frac{\pi}{3} + \frac{2k\pi}{3}$$

for $k = 0, 1, 2$. So they are

$$\theta = \frac{\pi}{3},\ \pi,\ \frac{5\pi}{3}.$$

Write out the solutions. It is convenient to label them as z_k; that is, z_0, z_1, z_2.

Thus the solutions of the equation are

$$z_0 = 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right),$$
$$z_1 = 3\,(\cos\pi + i\sin\pi),$$
$$z_2 = 3\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right).$$

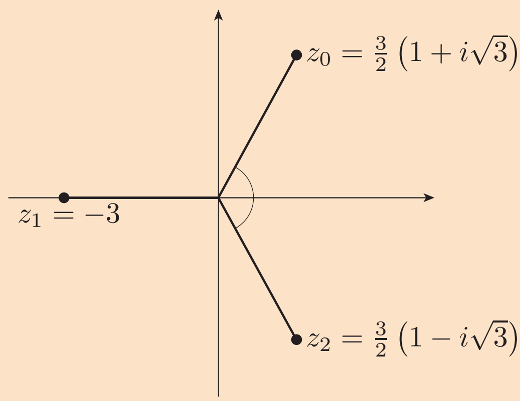
We can write z_2 using its principal argument as follows:

$$z_2 = 3\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right).$$

In Cartesian form, we have

$$z_0 = \tfrac{3}{2}(1 + i\sqrt{3}), \quad z_1 = -3, \quad z_2 = \tfrac{3}{2}(1 - i\sqrt{3}).$$

A sketch of the solutions on the complex plane is given below.



In Worked Exercise A34 we took $k = 0, 1, 2$ in the formula

$$\theta = \frac{\pi}{3} + \frac{2k\pi}{3},$$

and obtained three corresponding solutions z_0, z_1, z_2. Notice that if we take $k = 3$ in the formula, then we obtain

$$\theta = \frac{\pi}{3} + \frac{6\pi}{3} = \frac{\pi}{3} + 2\pi,$$

which gives solution z_0 again, since this value of θ differs from the

argument of z_0 by an integer multiple of 2π. You can check in the same way that if we take $k = 4$ then we obtain solution z_1 again, and if we take $k = 5$ then we obtain solution z_2 again, and so on. That is, if we take $k = 0, 1, 2, 3, 4, \ldots$, in Worked Exercise A34, then after the third different solution the solutions repeat in an indefinite cycle. The same solutions are repeated if we take k to be a negative integer.

We can use the method of Worked Exercise A34 to find the solutions of any complex equation of the form

$$z^n = a,$$

where a is a known complex number. To do this, we start by writing both z and a in polar form so that, say,

$$z = r(\cos\theta + i\sin\theta) \quad \text{and} \quad a = \rho(\cos\phi + i\sin\phi),$$

where r and θ are variables whose values we must find, and ρ and ϕ are known real numbers.

Then, by de Moivre's Theorem, the equation $z^n = a$ can be written as

$$r^n(\cos n\theta + i\sin n\theta) = \rho(\cos\phi + i\sin\phi).$$

Hence we must have $r^n = \rho$, so $r = \rho^{1/n}$. Also $n\theta$ must represent the same angle as ϕ. We again use the fact that a complex number has many arguments, so adding any integer multiple of 2π to the argument ϕ of a gives the same complex number a. So we have

$$n\theta = \phi + 2k\pi, \quad \text{for any integer } k,$$

that is,

$$\theta = \frac{\phi}{n} + \frac{2k\pi}{n}, \quad \text{for any integer } k.$$

If $k = n$ we have $\theta = \phi/n + 2\pi$, which represents the same angle as ϕ/n. So taking $k = 0, 1, 2, \ldots, n-1$ will give the n different solutions of the equation $z^n = a$.

Exercise A77

(a) Use the method described above to find the six solutions of the equation $z^6 = 1$ in polar form using the principal argument.

(b) Sketch the position of each solution in the complex plane.

(c) Write down the Cartesian form of each solution.

In Exercise A77 you found the solutions of the equation $z^6 = 1$. These are known as the sixth roots of unity, and in the complex plane they are equally spaced around the circle of radius 1, centre the origin. More generally, the solutions of the equation $z^n = 1$ are known as the **nth roots of unity**, and in the complex plane they are equally spaced around the circle of radius 1, centre the origin. For any $n \in \mathbb{N}$, the real number 1 is always one of the nth roots of unity.

The nth roots of any complex number are also equally spaced around a circle with centre the origin, but the circle may not have radius 1 and there may not be a root on the real axis, as the following exercises illustrate.

Exercise A78

Solve the equation $z^4 = -4$, expressing your answers in Cartesian form. Mark your solutions on a diagram of the complex plane.

Exercise A79

Solve the equation $z^3 = 8i$, expressing your answers in Cartesian form. Mark your solutions on a diagram of the complex plane.

The next box summarises the method we have been using by giving a formula for the roots of a complex number.

Roots of a complex number

Let $a = \rho(\cos\phi + i\sin\phi)$ be a complex number in polar form. Then, for any $n \in \mathbb{N}$, the equation $z^n = a$ has n solutions, given by

$$z = \rho^{1/n}\left(\cos\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right) + i\sin\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right)\right),$$

for $k = 0, 1, \ldots, n-1$.

This result gives the n solutions of any equation of the form $z^n = a$, where a is a non-zero complex number. Now the equation $z^n = a$, which can be written as $z^n - a = 0$, is an example of a polynomial equation whose coefficients, 1 and $-a$, are complex numbers. Other examples of polynomial equations with complex coefficients are

$$z^2 + (1+i)z + i = 0$$

and

$$(1+i)z^5 + 2iz^3 - 3z^2 + (1-2i)z - 1 = 0.$$

It can be shown that the following result holds; the proof is not included in this module.

Theorem A5 The Fundamental Theorem of Algebra

Every polynomial equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0,$$

where $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{C}$ and $a_n \neq 0$, has at least one solution in $\mathbb{C}$.

We say that a number system is **algebraically closed** if every polynomial equation with coefficients in this system has a solution in this system. Therefore, unlike the reals and the rationals, the complex numbers are an algebraically closed system of numbers.

In 1799 Carl Friedrich Gauss (1777–1855), one of the greatest mathematicians of all time, published what is often considered to be the first satisfactory proof of the Fundamental Theorem of Algebra. However, Gauss himself was not satisfied with the proof and over the course of the next fifty years published three further proofs. Later Gauss's original proof, which was mainly geometrical, was shown to be incomplete. In 1920 the gap in Gauss's proof was filled by the Russian mathematician Alexander Ostrowski (1893–1986).

Carl Friedrich Gauss

Alexander Ostrowski

Although we know from the Fundamental Theorem of Algebra that every polynomial equation with coefficients in $\mathbb{C}$ has at least one solution in $\mathbb{C}$, finding solutions of such polynomial equations is not easy. However, there are a few theorems that can help us do this in some special cases.

One of these theorems is the Factor Theorem (Theorem A2), which you met for polynomials where the number system is $\mathbb{R}$ in Subsection 1.4, but is also true if the number system is $\mathbb{C}$, as stated below.

Theorem A6 Factor Theorem (in $\mathbb{C}$)

Let $p(z)$ be a polynomial with coefficients in $\mathbb{C}$, and let $\alpha \in \mathbb{C}$. Then $p(\alpha) = 0$ if and only if $z - \alpha$ is a factor of $p(z)$.

In this statement of the theorem, the letter z has been used in place of x, as this is the label usually used for a complex variable. The proof is otherwise exactly the same as the proof of the theorem in $\mathbb{R}$, which you will see in Unit A3.

The next theorem is also useful. It can be deduced from the Fundamental Theorem of Algebra and the Factor Theorem. The proof of this follows in a similar way to the proof of Theorem A3 that you will see in Unit A3.

Theorem A7

Every polynomial

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0,$$

where $n \geq 1$ and the coefficients are in $\mathbb{C}$, with $a_n \neq 0$, has a factorisation

$$p(z) = a_n(z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_n),$$

where the complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots (not necessarily distinct) of $p(z)$.

Together Theorems A5 and A7 tell us that a polynomial equation of degree n with coefficients in $\mathbb{C}$ has at least one solution in $\mathbb{C}$, but can have no more than n solutions (all in $\mathbb{C}$). Moreover, if 'repeated' solutions are counted separately, then a polynomial equation of degree n with coefficients in $\mathbb{C}$ has *exactly* n solutions (all in $\mathbb{C}$). For example, the polynomial equation

$$(z-1)^3(z+4)^2(z-i) = 0$$

has degree six and has exactly six solutions: the solution 1 is counted three times, the solution -4 is counted twice and the solution i is counted once.

A third result that can help us find solutions of polynomial equations in some special cases is Theorem A8 below. You may have noticed that it follows from the quadratic formula that, for a quadratic polynomial with *real* coefficients, the roots are either both real or they occur as a complex conjugate pair.

More generally, we have the following result.

Theorem A8

If $p(z)$ is a polynomial with *real* coefficients, then whenever α is a complex root of p, so is $\overline{\alpha}$.

This result is not proved here, but you might like to try to prove it yourself; it is included as a 'challenging' exercise in the additional exercises booklet for this unit. In addition, the factors $z - \alpha$ and $z - \overline{\alpha}$ of $p(z)$ can be combined to give a real quadratic factor of $p(z)$, namely

$$(z - \alpha)(z - \overline{\alpha}) = z^2 - (\alpha + \overline{\alpha})z + \alpha\overline{\alpha},$$

which has real coefficients, since $\alpha + \overline{\alpha} = 2\operatorname{Re}\alpha$ and $\alpha\overline{\alpha} = |\alpha|^2$.

Worked Exercise A35

(a) Show that $z = i$ is a root of the polynomial

$$p(z) = z^4 - 3z^3 + 2z^2 - 3z + 1.$$

(b) Hence find all the roots of $p(z)$.

Solution

(a) Check that $p(i) = 0$.

We have

$$\begin{aligned} p(i) &= i^4 - 3i^3 + 2i^2 - 3i + 1 \\ &= 1 + 3i - 2 - 3i + 1 \\ &= 0, \end{aligned}$$

so i is a root of $p(z)$.

(b) The polynomial $p(z)$ has *real* coefficients, so for each complex root α, the complex conjugate $\overline{\alpha}$ is also a root.

Since p has real coefficients, $z = -i$ is also a root of $p(z)$, so $(z - i)(z + i) = z^2 + 1$ is a factor of $p(z)$.

We have $z^4 - 3z^3 + 2z^2 - 3z + 1 = (z^2 + 1)(az^2 + bz + c)$. Equating the coefficients of z^4, z^3 and the constant term in this equation gives $a = 1$, $b = -3$ and $c = 1$.

By equating coefficients, we obtain

$$z^4 - 3z^3 + 2z^2 - 3z + 1 = (z^2 + 1)(z^2 - 3z + 1).$$

So the remaining two roots of $p(z)$ are the solutions of the equation $z^2 - 3z + 1 = 0$.

Using the quadratic formula, we have

$$z = \frac{3 \pm \sqrt{9 - 4}}{2} = \frac{3 \pm \sqrt{5}}{2}.$$

Hence the four roots of $p(z)$ are i, $-i$, $\frac{1}{2}(3 + \sqrt{5})$ and $\frac{1}{2}(3 - \sqrt{5})$.

Exercise A80

(a) Show that $z = 2i$ is a root of the polynomial

$$p(z) = z^4 - 2z^3 + 7z^2 - 8z + 12.$$

(b) Hence find all the roots of $p(z)$.

Exercise A81

Find, in the form $a_n z^n + \cdots + a_1 z + a_0$, a polynomial whose roots are 1, -2, $3i$ and $-3i$.

2.5 The complex exponential function

The real exponential function $f(x) = e^x$, also written as $f(x) = \exp x$, has the following properties:

$$e^0 = 1, \quad e^x e^y = e^{x+y}, \quad 1/e^x = e^{-x}, \quad \text{for all } x, y \in \mathbb{R}.$$

We will consider the real function $f(x) = e^x$ in more detail in the analysis units (Books D and F), but here we extend the definition of this function to define a function $f(z) = e^z$ whose domain and codomain are $\mathbb{C}$.

We expect complex powers of e to satisfy the same basic properties as real powers of e. So, for example, we expect that

$$e^{z_1}e^{z_2} = e^{z_1+z_2} \quad \text{and} \quad 1/e^z = e^{-z}, \quad \text{for all } z, z_1, z_2 \in \mathbb{C}.$$

It turns out that, if this is to be achieved, then the definition of e^z has to be as follows.

Definition

If $z = x + iy$, then $e^z = e^x(\cos y + i \sin y)$.

Worked Exercise A36

Use the definition above to show that

$$e^{z_1}e^{z_2} = e^{z_1+z_2}$$

for all complex numbers z_1 and z_2.

Solution

We multiply moduli and add angles in polar form.

Suppose that $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$.

Since x_1, x_2, y_1 and y_2 are *real* numbers, the usual exponential rules apply to them.

Then, using the trigonometric identities from Subsection 2.3, we have

$$\begin{aligned}
e^{z_1}e^{z_2} &= e^{x_1}(\cos y_1 + i \sin y_1)e^{x_2}(\cos y_2 + i \sin y_2) \\
&= e^{x_1}e^{x_2}(\cos y_1 + i \sin y_1)(\cos y_2 + i \sin y_2) \\
&= e^{x_1+x_2}(\cos y_1 \cos y_2 + i^2 \sin y_1 \sin y_2 \\
&\qquad\qquad + i \cos y_1 \sin y_2 + i \sin y_1 \cos y_2) \\
&= e^{x_1+x_2}(\cos y_1 \cos y_2 - \sin y_1 \sin y_2 \\
&\qquad\qquad + i(\cos y_1 \sin y_2 + \sin y_1 \cos y_2)) \\
&= e^{x_1+x_2}(\cos(y_1 + y_2) + i \sin(y_1 + y_2)) \\
&= e^{(x_1+x_2)+i(y_1+y_2)} = e^{(x_1+iy_1)+(x_2+iy_2)} \\
&= e^{z_1+z_2}.
\end{aligned}$$

Exercise A82

(a) Using the definition for e^z above and de Moivre's Theorem (Theorem A4), show that

$$\frac{1}{e^z} = e^{-z}, \quad \text{for all } z \in \mathbb{C}.$$

(b) Use the results from part (a) and Worked Exercise A36 to show that $e^{z_1}/e^{z_2} = e^{z_1 - z_2}$, for all $z_1, z_2 \in \mathbb{C}$.

So the rules for multiplication and division of complex powers of e are exactly the same as those for real powers. Furthermore, when the exponent z is real, that is when $z = x + 0i$, where $x \in \mathbb{R}$, the definitions of a real and a complex power of e coincide, since

$$e^z = e^{x+i0} = e^x(\cos 0 + i \sin 0) = e^x.$$

On the other hand, if $z = 0 + iy$, where $y \in \mathbb{R}$, then the definition gives the following formula.

Euler's Formula

$$e^{iy} = \cos y + i \sin y.$$

Putting $y = \pi$ in Euler's Formula, we obtain

$$e^{i\pi} = \cos \pi + i \sin \pi = -1 + i0 = -1.$$

This equation is usually written as follows.

Euler's Identity

$$e^{i\pi} + 1 = 0.$$

This is a remarkable relationship between five important numbers: 0, 1, i, π and e.

In 1748, Leonhard Euler, in his famous *Introductio in analysin infinitorum* (Introduction to the Analysis of the Infinite), published the equations:

$$e^{+v\sqrt{-1}} = \cos v + \sqrt{-1}\sin v,$$

and

$$e^{-v\sqrt{-1}} = \cos v - \sqrt{-1}\sin v.$$

However, Euler himself never published what we now know as Euler's Identity.

Euler was also responsible for introducing the symbol i for the imaginary number with the property that $i^2 = -1$, and the symbol e to represent the base of natural logarithms, although he did not use the symbol i until 1777 and it was not published until 1794.

The formula $e^{iy} = \cos y + i \sin y$ gives us an alternative form for the expression of a complex number in polar form. If

$$z = x + iy = r(\cos\theta + i\sin\theta),$$

then we can write $\cos\theta + i\sin\theta$ as $e^{i\theta}$, so

$$z = re^{i\theta}.$$

A complex number expressed in this way is said to be in *exponential form*.

Definition

A non-zero complex number $z = x + iy = r(\cos\theta + i\sin\theta)$ is in **exponential form** if it is expressed as

$$z = re^{i\theta}.$$

Rather than using the term *exponential form*, some texts regard $re^{i\theta}$ as another version of *polar form*, since it involves the modulus and angle of the complex number.

When we use exponential form for complex numbers, de Moivre's Theorem (Theorem A4) becomes the simple result

$$(e^{i\theta})^n = e^{in\theta}, \quad \text{for all } \theta \in \mathbb{R} \text{ and all } n \in \mathbb{Z}.$$

Similarly, if $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, the rules for multiplying and dividing complex numbers become the following simple results:

$$z_1 z_2 = r_1 e^{i\theta_1} \times r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1+\theta_2)},$$

$$\frac{z_1}{z_2} = \frac{r_1 e^{i\theta_1}}{r_2 e^{i\theta_2}} = \frac{r_1}{r_2} e^{i(\theta_1-\theta_2)} \quad (\text{provided } z_2 \neq 0).$$

There is also a useful formula for the complex conjugate of a complex number in exponential form, as follows.

If $z = re^{i\theta}$, then $\overline{z} = re^{-i\theta}$.

This formula can be proved as follows. If $z = re^{i\theta}$, then $z = r(\cos\theta + i\sin\theta)$, so

$$\begin{aligned}\overline{z} &= r(\cos\theta - i\sin\theta)\\ &= r(\cos(-\theta) + i\sin(-\theta))\\ &= re^{-i\theta}.\end{aligned}$$

The second line here follows from the trigonometric identities $\cos(-\theta) = \cos\theta$ and $\sin(-\theta) = -\sin\theta$.

Exercise A83

Use Euler's Identity to prove that if $z = re^{i\theta}$, then $-z = re^{i(\theta+\pi)}$.

2.6 Summary: Cartesian, polar and exponential form

You have seen in the previous subsections that certain calculations with complex numbers are considerably easier in some forms than in others. For example, if we use polar form or exponential form, then we can easily find powers using de Moivre's Theorem (Theorem A4). Here is a summary of the main features of the different forms of a complex number, and how to convert between them.

Let

$$\begin{aligned}z &= x + iy = r(\cos\theta + i\sin\theta) = re^{i\theta},\\ z_1 &= x_1 + iy_1 = r_1(\cos\theta_1 + i\sin\theta_1) = r_1e^{i\theta_1},\\ z_2 &= x_2 + iy_2 = r_2(\cos\theta_2 + i\sin\theta_2) = r_2e^{i\theta_2}.\end{aligned}$$

Complex conjugate

Cartesian form $\overline{z} = x - iy$

Polar form $\overline{z} = r(\cos\theta - i\sin\theta)$

Exponential form $\overline{z} = re^{-i\theta}$

Product

Cartesian form Use the usual rules of arithmetic to find z_1z_2.

Polar form $z_1z_2 = r_1r_2\left(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\right)$

Exponential form $z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}$

Reciprocal (In each case, $z \neq 0$.)

Cartesian form $\dfrac{1}{z} = \dfrac{1}{z} \times \dfrac{\overline{z}}{\overline{z}} = \dfrac{\overline{z}}{|z|^2}$

Polar form $\dfrac{1}{z} = \dfrac{1}{r}(\cos(-\theta) + i\sin(-\theta)) = \dfrac{1}{r}(\cos\theta - i\sin\theta)$

Exponential form $\dfrac{1}{z} = \dfrac{1}{r}e^{-i\theta}$

Quotient (In each case, $z_2 \neq 0$.)

Cartesian form $\dfrac{z_1}{z_2} = \dfrac{z_1}{z_2} \times \dfrac{\overline{z_2}}{\overline{z_2}} = \dfrac{z_1\overline{z_2}}{|z_2|^2}$

Polar form $\dfrac{z_1}{z_2} = \dfrac{r_1}{r_2}(\cos(\theta_1-\theta_2) + i\sin(\theta_1-\theta_2))$

Exponential form $\dfrac{z_1}{z_2} = \dfrac{r_1}{r_2}e^{i(\theta_1-\theta_2)}$

Converting polar and exponential form to Cartesian form

Use the equations

$$x = r\cos\theta, \quad y = r\sin\theta.$$

Converting Cartesian form to polar and exponential form

Find the modulus r, using $r = |z| = \sqrt{x^2+y^2}$.

Mark z on a sketch of the complex plane. Find the acute angle ϕ at the origin in the right-angled triangle formed by drawing the perpendicular from z to the real axis, using

$$\cos\phi = \frac{|x|}{r}.$$

Hence find the principal argument.

3 Modular arithmetic

In this section you will see how we can do arithmetic with finite sets of integers. We do this by using *modular arithmetic*, which you should have met in your previous studies. This type of arithmetic is important in number theory (the study of the integers) and in cryptography. You will use it frequently in the group theory units of this module (Books B and E).

3.1 The Division Theorem

If we divide one positive integer by another we obtain a *quotient* and a *remainder*. For example, 29 divided by 4 gives quotient 7 and remainder 1 because $29 = 7 \times 4 + 1$. If we divide any positive integer by 4, the remainder will be one of the numbers 0, 1, 2, 3.

This idea can be extended to the division of a negative integer by a positive integer. For example, -19 divided by 4 gives quotient -5 and remainder 1 because $-19 = (-5) \times 4 + 1$. If we divide any negative integer by 4, the remainder is again one of the numbers 0, 1, 2, 3.

This result can be generalised to the following theorem.

Theorem A9 Division Theorem

Let a and n be integers, with $n > 0$. Then there are unique integers q and r such that

$$a = qn + r, \quad \text{with } 0 \leq r < n.$$

We say that dividing a by the **divisor** n gives the **quotient** q and **remainder** r.

A formal proof of Theorem A9 is not given here, but the theorem can be illustrated as follows. We mark integer multiples of n along the real line as shown in Figure 16, and then observe in which of the resulting intervals of length n the integer a lies. Suppose that a lies in the interval $[qn, (q+1)n)$, so that $qn \leq a < (q+1)n$, as illustrated.

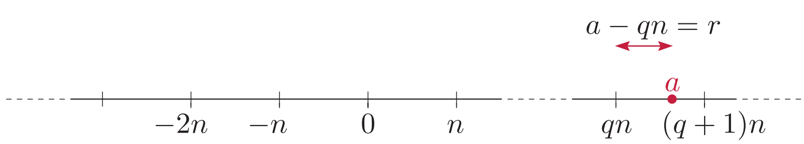


Figure 16 The number a in the interval $[qn, (q+1)n)$

Then, if we let $r = a - qn$, we have $a = qn + r$ and $0 \leq r < n$, which is the required result.

Exercise A84

For each of the following integers a and n, find the quotient and remainder on division of a by n.

(a) $a = 65, \quad n = 7$ (b) $a = -256, \quad n = 13$

Exercise A85

(a) What are the possible remainders on division of an integer by 7?

(b) Find two positive and two negative integers all of which have remainder 3 on division by 7.

3.2 Congruence

The Division Theorem (Theorem A9) tells us that, when we divide any integer by a positive integer n, the set of possible remainders is $\{0, 1, 2, \ldots, n-1\}$. Integers that differ by a multiple of n have the same remainder on division by n and are, in this sense, 'the same' as each other. We now introduce some notation and terminology for this idea of 'sameness', which is known as *congruence*.

Definitions

Let n be a positive integer. Two integers a and b are **congruent modulo n** if $a - b$ is a multiple of n; that is, if a and b have the same remainder on division by n.

In symbols we write

$$a \equiv b \pmod{n}.$$

Such a statement is called a **congruence**, and n is called the **modulus** of the congruence.

The word 'modulus' here has a different meaning from its use to mean the 'size' of a real number or a complex number. This different usage reminds us that it is always important to interpret technical terms according to their context.

We read '$a \equiv b \pmod{n}$' as 'a is congruent to b modulo n'.

The terms 'congruent' and 'modulus', together with the symbol for congruence, all appear for the first time in Gauss's classic text *Disquisitiones Arithmeticae* (Arithmetical Investigations) of 1801, the work which, in the words of historian Olaf Neumann, 'transformed number theory from a scattering of islands into an established continent of mathematics.'

Worked Exercise A37

Which of the following congruences are true, and which are false?

(a) $27 \equiv 5 \pmod{11}$ (b) $14 \equiv -6 \pmod{3}$

(c) $343 \equiv 207 \pmod{68}$ (d) $1 \equiv -1 \pmod{2}$

Solution

It is often simplest to check a congruence $a \equiv b \pmod{n}$ by considering the difference $a - b$.

(a) $27 - 5 = 22$, which is a multiple of 11, so this congruence is true.

Alternatively, $27 = 2 \times 11 + 5$ and $5 = 0 \times 11 + 5$, so 27 and 5 both have remainder 5 on division by 11.

(b) $14 - (-6) = 20$, which is not a multiple of 3, so this congruence is false.

Alternatively, $14 = 4 \times 3 + 2$ and $-6 = (-2) \times 3 + 0$, so 14 has remainder 2 on division by 3, but -6 has remainder 0.

(c) $343 - 207 = 136 = 2 \times 68$, so this congruence is true.

Alternatively, $343 = 5 \times 68 + 3$ and $207 = 3 \times 68 + 3$, so 343 and 207 both have remainder 3 on division by 68.

(d) $1 - (-1) = 2$, so this congruence is true.

Alternatively, both 1 and -1 have remainder 1 on division by 2.

Exercise A86

Find the remainder on division by 17 of each of the numbers 25, 53, -15, 3 and 127, and state any congruences modulo 17 that exist between these numbers.

We shall need to use some properties of congruences in the following sections, so we state these properties here. This may seem a long list, but these properties are quite simple; in fact, they are what you might expect.

Theorem A10 Properties of congruences

Let n and m be positive integers, and let a, b, c, d be integers. The following properties hold.

Reflexivity $a \equiv a \pmod{n}$.

Symmetry If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Transitivity If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Addition If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

Multiplication If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Powers If $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$.

To see why these properties hold, we use the definition of congruence: two integers a and b are congruent modulo n if $a - b$ is a multiple of n.

The reflexive property holds because $a - a = 0 = 0 \times n$, so we have $a \equiv a \pmod{n}$.

To see why the symmetric property holds, suppose that $a \equiv b \pmod{n}$, so $a - b = kn$ for some integer k. But $b - a = -(a - b)$, so $b - a = (-k)n$. Since $-k$ is also an integer, it follows that $b \equiv a \pmod{n}$.

We can see that the transitive property holds in a similar way. Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $a - b = kn$ and $b - c = ln$ for some integers k and l. Hence

$$a - c = a - b + b - c = kn + ln = (k + l)n.$$

Since $k + l$ is an integer, it follows that $a \equiv c \pmod{n}$.

In the next worked exercise we prove that the addition property holds, and you are asked to prove the multiplication property in Exercise A87.

Worked Exercise A38

Prove that the addition property for congruences holds:

$$\text{if } a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n}, \text{ then } a + c \equiv b + d \pmod{n}.$$

Solution

Suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a - b = kn$ and $c - d = ln$ for some integers k and l. Hence $a = b + kn$ and $c = d + ln$, so

$$a + c = b + kn + d + ln = b + d + (k + l)n.$$

Therefore $(a + c) - (b + d) = (k + l)n$. Since $k + l$ is an integer, it follows that $a + c \equiv b + d \pmod{n}$. Thus the addition property holds.

Exercise A87

Prove that the multiplication property for congruences holds:

if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

The powers property is obtained by applying the multiplication property repeatedly. Suppose that $a \equiv b \pmod{n}$. Then the multiplication property gives

$$a^2 \equiv b^2 \pmod{n}.$$

We can now apply the multiplication property to

$$a \equiv b \pmod{n} \quad \text{and} \quad a^2 \equiv b^2 \pmod{n}.$$

to obtain

$$a^3 \equiv b^3 \pmod{n}.$$

Continuing in this way, we obtain

$$a^m \equiv b^m \pmod{n} \text{ for any } m \in \mathbb{N},$$

which is the powers property.

The properties of congruences in Theorem A10 are particularly useful when we want to find the remainder of a large integer on division by another integer, as the next worked exercise illustrates.

Worked Exercise A39

(a) Find the remainders of both 2375 and 5421 on division by 22.

(b) Find the remainder of 2375×5421 on division by 22.

(c) Find the remainder of $(2375)^{15}$ on division by 22.

Solution

(a) Start with 2375 and subtract or add convenient multiples of 22 until you reach an integer in $\{0, 1, 2, \ldots, 21\}$. Here we can subtract 2200, then 110, then 66, then add 22.

Using the transitivity property of congruences we obtain

$$2375 \equiv 175 \equiv 65 \equiv -1 \equiv 21 \pmod{22}.$$

Do the same for 5421. We can subtract 4400, then 880, then 110, then 22.

Similarly,

$$5421 \equiv 1021 \equiv 141 \equiv 31 \equiv 9 \pmod{22}.$$

So 2375 has remainder 21 on division by 22, and 5421 has remainder 9 on division by 22.

(b) Use the multiplication property. Find integers congruent modulo 22 to 2375 and 5421 that are easier to multiply.

Using the multiplication property of congruences and the answer to part (a), we obtain

$$2375 \times 5421 \equiv 21 \times 9 \equiv -1 \times 9 \equiv -9 \equiv 13 \pmod{22},$$

so 2375×5421 has remainder 13 on division by 22.

(c) Use the powers property. Find an integer congruent modulo 22 to 2375 whose powers are easier to find.

Using the powers property of congruences and the answer to part (a), we obtain

$$(2375)^{15} \equiv 21^{15} \equiv (-1)^{15} \equiv -1 \equiv 21 \pmod{22},$$

so $(2375)^{15}$ has remainder 21 on division by 22.

The worked exercise above shows that there is a real advantage in using congruences, since the number $(2375)^{15}$ is too large to fit into the memory of most computers.

Exercise A88

(a) Find the remainder of both 3869 and 1685 on division by 16.

(b) Find the remainder of $3869 + 1685$ on division by 16.

(c) Find the remainder of $(3869 + 1685)^4$ on division by 16, and hence find the remainder of $(3869 + 1685)^{111}$ on division by 16.

3.3 Operations in $\mathbb{Z}_n$

The Division Theorem (Theorem A9) tells us that all the possible remainders on dividing an integer by a positive integer n lie in the set

$$\{0, 1, \ldots, n-1\}.$$

We denote this set by $\mathbb{Z}_n$. For each integer $n \geq 2$ we have a set $\mathbb{Z}_n$, and it is on these sets that we perform *modular arithmetic*. The modular addition operations $+_n$ and modular multiplication operations $\times_n$ are defined as follows.

Definitions

For any integer $n \geq 2$,

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

For a and b in $\mathbb{Z}_n$, the operations $+_n$ and $\times_n$ are defined by:

$a +_n b$ is the remainder of $a + b$ on division by n;

$a \times_n b$ is the remainder of $a \times b$ on division by n.

The integer n is called the **modulus** for this arithmetic.

We read $a +_n b$ as 'a plus b, mod n', and $a \times_n b$ as 'a times b, mod n'.

For example, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and we have

$3 + 6 = 9, \quad \text{so } 3 +_7 6 = 2,$

$3 \times 6 = 18, \quad \text{so } 3 \times_7 6 = 4.$

You have certainly met some modular arithmetic before, as the operations $+_{12}$ and $+_{24}$ are used in measuring time on 12-hour and 24-hour clocks, respectively.

Arithmetic carried out on the elements of the set $\mathbb{Z}_n$ using the operations $+_n$ and $\times_n$ is called **arithmetic modulo** n.

Exercise A89

Evaluate the following.

(a) $3 +_5 2$ (b) $4 +_{17} 5$ (c) $8 +_{16} 12$

(d) $3 \times_5 2$ (e) $4 \times_{17} 5$ (f) $8 \times_{16} 12$

You can often use the properties of congruences to help you carry out arithmetic modulo n efficiently, without using a calculator, as demonstrated in the next worked exercise. There are usually many different ways to proceed.

Worked Exercise A40

Evaluate the following.

(a) $29 \times_{31} 18$ (b) $12 \times_{26} 15$

Solution

(a) Use the fact that $29 \equiv -2 \pmod{31}$, and it is easier to multiply by -2 than by 29. Remember that the final answer needs to be an integer in $\mathbb{Z}_{31}$.

We have

$$\begin{aligned} 29 \times 18 &\equiv -2 \times 18 \\ &\equiv -36 \\ &\equiv -5 \\ &\equiv 26 \pmod{31}. \end{aligned}$$

Thus $29 \times_{31} 18 = 26$.

(b) Use the fact that to multiply by 12, we can first multiply by 2 and then by 6. The final answer needs to be an integer in $\mathbb{Z}_{26}$.

We have

$$\begin{aligned} 12 \times 15 &\equiv 6 \times 2 \times 15 \\ &\equiv 6 \times 30 \\ &\equiv 6 \times 4 \\ &\equiv 24 \pmod{26}. \end{aligned}$$

Thus $12 \times_{26} 15 = 24$.

Exercise A90

Calculate the following without using a calculator.

(a) $7 \times_{27} 26$ (b) $16 \times_{29} 14$ (c) $9 \times_{33} 15$ (d) $37 \times_{45} 23$

(e) $15 \times_{34} 6$ (f) $9 \times_{40} 18$

In Subsection 1.2 you met a list of eleven properties that are satisfied by the set $\mathbb{Q}$ of rational numbers, the set $\mathbb{R}$ of real numbers and the set $\mathbb{C}$ of complex numbers. You saw that since these three sets each satisfy all eleven properties (together with a trivial twelfth property), these sets are all *fields*. You also saw that the set $\mathbb{Z}$ of integers does not satisfy all eleven of these properties, and so is not a field. In the rest of this section we will investigate whether the sets $\mathbb{Z}_n$ satisfy these properties.

We will also investigate which equations in $\mathbb{Z}_n$ have solutions; for example, do the equations

$$x +_{12} 5 = 2, \quad 5 \times_{12} x = 7, \quad 4 \times_{12} x = 6$$

have solutions? These may look much simpler than the equations we were trying to solve in $\mathbb{C}$, but they pose interesting questions. We shall see that the answers may depend on the modulus that we are using.

Before we consider these questions further, we look at addition and multiplication tables, which provide a convenient way of studying addition and multiplication in $\mathbb{Z}_n$.

We consider addition first. Here are the addition tables for $\mathbb{Z}_4$ and $\mathbb{Z}_7$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

In order to evaluate $4 +_7 2$, say, we look in the second table at the row labelled 4 and the column labelled 2 to obtain the answer 6.

Exercise A91

(a) Use the tables above to solve the following equations.

(i) $x +_4 3 = 2$. (ii) $x +_7 5 = 2$. (iii) $x +_4 2 = 0$. (iv) $x +_7 5 = 0$.

(b) What patterns do you notice in the tables?

Exercise A92

(a) Construct the addition table for $\mathbb{Z}_6$.

(b) Solve the equations $x +_6 1 = 5$ and $x +_6 5 = 1$.

For every integer $n \geq 2$, the additive properties of $\mathbb{Z}_n$ are the same as the additive properties of $\mathbb{R}$, as follows.

Addition in $\mathbb{Z}_n$ ($n \geq 2$)

A1 Closure For all $a, b \in \mathbb{Z}_n$,

$$a +_n b \in \mathbb{Z}_n.$$

A2 Associativity For all $a, b, c \in \mathbb{Z}_n$,

$$(a +_n b) +_n c = a +_n (b +_n c).$$

A3 Additive identity For all $a \in \mathbb{Z}_n$,

$$a +_n 0 = a = 0 +_n a.$$

A4 Additive inverses For each $a \in \mathbb{Z}_n$, there is a number $b \in \mathbb{Z}_n$ such that

$$a +_n b = 0 = b +_n a.$$

A5 Commutativity For all $a, b \in \mathbb{Z}_n$,

$$a +_n b = b +_n a.$$

The closure property (A1) follows because $a +_n b$ is the remainder on dividing $a + b$ by n, which, from the Division Theorem (Theorem A9), is in $\mathbb{Z}_n$.

The other properties can be deduced from the corresponding properties for integers. For example, we can see that the associativity property (A2) holds as follows. By definition, $(a +_n b) +_n c$ and $a +_n (b +_n c)$ are the remainders of the integers $(a + b) + c$ and $a + (b + c)$, respectively, on division by n. Since ordinary addition is associative, we have $(a + b) + c = a + (b + c)$, so

$$(a +_n b) +_n c = a +_n (b +_n c).$$

Exercise A93

By using the corresponding property for integers, prove that the commutativity property (A5) holds for $\mathbb{Z}_n$.

The additive inverses property (A4) states that *every* element of $\mathbb{Z}_n$ has an additive inverse in $\mathbb{Z}_n$. For example, 4 and 5 belong to $\mathbb{Z}_9$ and $4 +_9 5 = 0$, so 5 is an additive inverse of 4 in $\mathbb{Z}_9$ (and vice versa).

Additive inverses are sometimes written in the form $-_n a$; that is, if $a +_n b = 0$, then we write $b = -_n a$. For example, $5 = -_9 4$.

Exercise A94

(a) Use the addition table for $\mathbb{Z}_7$ (given earlier and repeated as Table 1) to complete the following table of additive inverses in $\mathbb{Z}_7$.

a	0	1	2	3	4	5	6
$-_7 a$							

(b) Complete the following table of additive inverses in $\mathbb{Z}_n$, justifying your answers.

a	0	1	2	...	r	...	$n-1$
$-_n a$							

Table 1

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Notice that each element a of $\mathbb{Z}_n$ has *exactly one* additive inverse in $\mathbb{Z}_n$, namely the integer obtained by subtracting a from n. For example, the additive inverse of 4 in $\mathbb{Z}_9$ is $9 - 4 = 5$.

The existence of additive inverses means that, as well as doing addition modulo n, we can also do **subtraction modulo** n. We define $a -_n b$ or, equivalently, $a - b \pmod{n}$, to be the remainder of $a - b$ on division by n.

For example, to find $2 -_{12} 5$, we have

$$2 - 5 = -3 \equiv 9 \pmod{12}.$$

Since $9 \in \mathbb{Z}_{12}$, it follows that

$$2 -_{12} 5 = 9.$$

3.4 Multiplicative inverses in $\mathbb{Z}_n$

In the last subsection it was stated that, for any integer $n \geq 2$, the set $\mathbb{Z}_n$ satisfies the same rules for addition modulo n as the real numbers satisfy for ordinary addition. When it comes to multiplication in $\mathbb{Z}_n$, *most* of the familiar rules for multiplication of the real numbers are true. In particular, the following properties hold.

Multiplication in $\mathbb{Z}_n$ ($n \geq 2$)

M1 Closure For all $a, b \in \mathbb{Z}_n$,

$$a \times_n b \in \mathbb{Z}_n.$$

M2 Associativity For all $a, b, c \in \mathbb{Z}_n$,

$$(a \times_n b) \times_n c = a \times_n (b \times_n c)$$

M3 Multiplicative identity For all $a \in \mathbb{Z}_n$,

$$a \times_n 1 = a = 1 \times_n a.$$

M5 Commutativity For all $a, b \in \mathbb{Z}_n$,

$$a \times_n b = b \times_n a.$$

The following property also holds.

Combining addition and multiplication in $\mathbb{Z}_n$ $(n \geq 2)$

D1 Distributivity For all $a, b, c \in \mathbb{Z}_n$,

$$a \times_n (b +_n c) = (a \times_n b) +_n (a \times_n c).$$

These properties can be shown to hold in a similar way to the additive properties. You will notice that one property is missing from the list of multiplicative properties, namely the multiplicative inverses property (M4).

We say that b is a **multiplicative inverse** of a in $\mathbb{Z}_n$ if $a, b \in \mathbb{Z}_n$ and $a \times_n b = b \times_n a = 1$. We now investigate the existence of multiplicative inverses.

Here are the multiplication tables for $\mathbb{Z}_4$ and $\mathbb{Z}_7$.

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

The table for $\mathbb{Z}_7$ shows that, for example, $3 \times_7 5 = 5 \times_7 3 = 1$, so 5 is a multiplicative inverse of 3 in $\mathbb{Z}_7$.

Exercise A95

(a) Use the tables above to answer the following.

- (i) Which elements of $\mathbb{Z}_4$ have multiplicative inverses?
- (ii) Find a multiplicative inverse of every element of $\mathbb{Z}_7$ except 0.

(b) Construct a multiplication table for $\mathbb{Z}_{10}$, and determine which elements of $\mathbb{Z}_{10}$ have multiplicative inverses.

In Exercise A95, you saw that, in contrast to $\mathbb{R}$ and $\mathbb{C}$, there are some values of n for which the number system $\mathbb{Z}_n$ contains non-zero elements that do not have a multiplicative inverse.

Before we investigate further the question of which elements of each number system $\mathbb{Z}_n$ have a multiplicative inverse, note that if an element of $\mathbb{Z}_n$ *does* have a multiplicative inverse, then it has *only one*. The multiplication tables for $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{10}$ show that this is true for these three number systems, but it is in fact true for any $\mathbb{Z}_n$, though this is less obvious than it is for additive inverses.

To see that it is true in general, suppose that a is an element of $\mathbb{Z}_n$, for some integer $n \geq 2$, and that both b and c are multiplicative inverses of a in $\mathbb{Z}_n$. Then

$$\begin{aligned} b &= 1 \times_n b \\ &= c \times_n a \times_n b \quad (\text{since } c \times_n a = 1) \\ &= c \times_n 1 \quad (\text{since } a \times_n b = 1) \\ &= c. \end{aligned}$$

That is, b and c are in fact the *same element* of $\mathbb{Z}_n$. Thus a has just one multiplicative inverse in $\mathbb{Z}_n$. We say that the inverse of a is *unique*.

When it exists, we denote the multiplicative inverse b of an element a of $\mathbb{Z}_n$ by a^{-1} and refer to it as *the* multiplicative inverse of a in $\mathbb{Z}_n$.

Notice also that if an element a of a number system $\mathbb{Z}_n$ has a multiplicative inverse b in $\mathbb{Z}_n$, then b also has a multiplicative inverse in $\mathbb{Z}_n$, namely a. This follows from the definition of a multiplicative inverse. For example, in $\mathbb{Z}_7$, the elements 3 and 5 are inverses of each other.

Let us now turn to the question of which elements of each number system $\mathbb{Z}_n$ have a multiplicative inverse. This question is connected with the *common factors* of a and n.

Definitions

Two integers a and b have a **common factor** c, where c is a natural number, if a and b are both divisible by c.

Two integers a and b are **coprime** (or **relatively prime**) if their only common factor is 1.

The **highest common factor** (**HCF**) of two integers a and b is their largest common factor.

If two integers a and b are coprime, we also say that a is coprime to b, or that b is coprime to a.

In some texts the highest common factor of a and b is called the 'greatest common divisor' (GCD).

It turns out that an element a of $\mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$ exactly when a and n are coprime. That is, if a and n are coprime, then a has a multiplicative inverse in $\mathbb{Z}_n$, but if a and n are not coprime, then a has no multiplicative inverse.

We prove this important result later in this subsection, but first we consider how to find multiplicative inverses where they exist. Of course, we could do this by trial and error, or by writing out the multiplication table for $\mathbb{Z}_n$, but for large values of n these methods are very cumbersome. Fortunately a more efficient method exists, based on *Euclid's Algorithm*.

Euclid's Algorithm is a method for finding the highest common factor of two positive integers, first described (albeit in a different form) in Euclid's *Elements*, which dates from around 300 BCE. Given an element a of $\mathbb{Z}_n$, we can apply Euclid's Algorithm to determine whether or not a and n are coprime; if they are coprime, then we know that a has a multiplicative inverse in $\mathbb{Z}_n$, but otherwise it does not. Moreover, if a and n *are* coprime, then we can use the equations that arise from applying Euclid's Algorithm to work out the multiplicative inverse of a, using a method known as **backwards substitution**.

Euclid's Algorithm proceeds by repeatedly applying the Division Theorem, as in the following example. Suppose we want to find the highest common factor of the integers 32 and 9. We start by dividing 32 by 9, which gives quotient 3 and remainder 5, as in the equation

$$32 = 3 \times 9 + 5.$$

Next, we divide 9 by 5, giving quotient 1, remainder 4 and the equation

$$9 = 1 \times 5 + 4.$$

We continue in this way, at each step forming a new equation by dividing the *divisor* from the previous equation by the *remainder* from that equation. The complete list of equations arising from Euclid's Algorithm in this example is given below.

$$\begin{aligned}
32 &= 3 \times 9 + 5 \\
9 &= 1 \times 5 + 4 \\
5 &= 1 \times 4 + 1 \\
4 &= 4 \times 1 + 0
\end{aligned}$$

We stop when the remainder is 0; giving us the last equation. We always eventually reach this stage, because the remainders decrease by at least 1 at each step. The remainder in the *second-to-last equation* is the highest common factor of the two integers we started with.

So, for example, the list of equations above shows that the highest common factor of 32 and 9 is 1; they are coprime. We conclude that the number 9 does have a multiplicative inverse in $\mathbb{Z}_{32}$.

Before we describe the process of backwards substitution and use it to find this inverse, let us see why Euclid's Algorithm works. Suppose we have two positive integers, say a_1 and a_2, and we apply the Division Theorem to obtain the equation

$$a_1 = qa_2 + a_3,$$

where $0 \leq a_3 < a_2$. This equation can be rearranged as

$$a_3 = a_1 - qa_2.$$

It follows from this rearranged equation that any integer that is a factor of both a_1 and a_2 (and so is a factor of $a_1 - qa_2$) must also be a factor of a_3. Thus any common factor of a_1 and a_2 is also a common factor of a_2 and a_3. Moreover, the unrearranged form of the equation tells us, by a similar argument, that any common factor of a_2 and a_3 must also be a common factor of a_1 and a_2. It follows that the highest common factor (HCF) of a_1 and a_2 is equal to the HCF of a_2 and a_3.

So, at each stage of Euclid's Algorithm, a pair of integers a_1, a_2 leads to another pair of integers a_2, a_3 with the same highest common factor. In the example above, we obtain the sequence of pairs

32 and 9,   9 and 5,   5 and 4,   4 and 1,   1 and 0,

and each pair has the same HCF.

The final pair of integers always has second integer 0, so its HCF is its first integer; this is the integer, say d, that appears as the remainder in the second-to-last equation. Since each pair has the same HCF, it follows that the HCF of the original pair is also d.

Euclid's Algorithm is much quicker to apply than to describe! Try it for yourself in the next exercise.

Exercise A96

Use Euclid's Algorithm to find the HCF of 201 and 81. Deduce whether or not the integer 81 has a multiplicative inverse in $\mathbb{Z}_{201}$.

If we have applied Euclid's Algorithm to find the HCF of two positive integers n and a with $n > a$, and found that the HCF is 1, we can then use the list of equations obtained from the algorithm to find the multiplicative inverse of a in $\mathbb{Z}_n$ using the method of **backwards substitution**.

To illustrate the method, let us apply it to our example of Euclid's Algorithm above: this will yield the multiplicative inverse of 9 in $\mathbb{Z}_{32}$.

The first step is to rearrange each of the equations from Euclid's Algorithm to make the remainders the subjects of the equations. (We do not need the last equation, the one with remainder 0.) This gives

$$\begin{aligned}5 &= 32 - 3 \times 9\\ 4 &= 9 - 1 \times 5\\ 1 &= 5 - 1 \times 4.\end{aligned}$$

Notice that the last equation above expresses 1 as the sum of a multiple of 5 and a multiple of 4. (One of the multiples is negative – here the multiple of 4. This will always be the case because our starting integers, here 32 and 9, are both positive.)

The goal of the backwards substitution process is to obtain an equation that expresses 1 as the sum of multiples of our original two positive integers, 32 and 9. (Again, one of these multiples must be negative.)

The backwards substitution process starts with the last equation from Euclid's Algorithm:

$$1 = 5 - 1 \times 4.$$

Next, we use the second-to-last equation from Euclid's Algorithm to substitute for the 4 in the right-hand side of this equation. We then simplify the resulting equation to express 1 as the sum of multiples of 9 and 5, like this

$$\begin{aligned}1 &= 5 - (9 - 1 \times 5)\\ &= (-1 \times 9) + (2 \times 5).\end{aligned}$$

Notice that, in simplifying the equation, we treat the 9 and 5 as if they were *variables*, in the same way that we would simplify the expression $x - (y - 1x)$ to give $-1y + 2x$.

Now we repeat the process, using the third-to-last equation to substitute for the 5 in the right-hand side of *this* equation, then simplifying again to express 1 as the sum of multiples of 32 and 9:

$$\begin{aligned}1 &= (-1 \times 9) + 2 \times (32 - 3 \times 9)\\ &= (2 \times 32) + (-7 \times 9).\end{aligned}$$

We continue in this way, working upwards through all the equations from Euclid's Algorithm. In this case, though, there are no more equations and we have reached our goal: an equation that expresses 1 as the sum of multiples of 32 and 9.

We are now only a few short steps from finding the multiplicative inverse of 9 in $\mathbb{Z}_{32}$.

First, we rearrange our final equation to obtain a multiple of the smaller of the two integers, 9, on the left-hand side, and a multiple of the larger integer, 32, together with the term +1, on the right-hand side:

$$(-7) \times 9 = (-2) \times 32 + 1.$$

Next, we note that it follows from this equation that

$$(-7) \times 9 \equiv 1 \pmod{32}.$$

Now $-7 \notin \mathbb{Z}_{32}$, but since $-7 \equiv 25 \pmod{32}$ and $25 \in \mathbb{Z}_{32}$, we have

$$25 \times 9 \equiv 1 \pmod{32},$$

that is

$$25 \times_{32} 9 = 1.$$

Thus we have shown that the multiplicative inverse of 9 in $\mathbb{Z}_{32}$ is 25; that is, $9^{-1} = 25$ in $\mathbb{Z}_{32}$.

We can check this as follows:

$$\begin{aligned} 25 \times 9 &= 225 \\ &= 7 \times 32 + 1, \end{aligned}$$

so $25 \times 9 \equiv 1 \pmod{32}$, as expected.

The next worked exercise gives another example of using this method to find a multiplicative inverse in a number system $\mathbb{Z}_n$. In this example the method is applied a little more efficiently.

Worked Exercise A41

Find the multiplicative inverse of 10 in $\mathbb{Z}_{27}$.

Solution

Apply Euclid's Algorithm to 27 and 10, stopping when the remainder 1 is obtained (since the final equation, with remainder 0, is not needed).

Applying Euclid's Algorithm gives

$$\begin{aligned} 27 &= 2 \times 10 + 7 \\ 10 &= 7 + 3 \\ 7 &= 2 \times 3 + 1. \end{aligned}$$

Apply backwards substitution – we can do so by mentally rearranging the equations above as we need them; the rearranged equations are $1 = 7 - 2 \times 3$, $3 = 10 - 7$ and $7 = 27 - 2 \times 10$.

Starting with the last equation, we have

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2(10 - 7) \\ &= -2 \times 10 + 3 \times 7 \\ &= -2 \times 10 + 3(27 - 2 \times 10) \\ &= 3 \times 27 - 8 \times 10. \end{aligned}$$

This final equation expresses 1 in terms of multiples of 27 and 10, and can be rearranged as $(-8) \times 10 = (-3) \times 27 + 1$.

Hence

$$(-8) \times 10 \equiv 1 \pmod{27}.$$

But $-8 \equiv 19 \pmod{27}$, so

$$19 \times 10 \equiv 1 \pmod{27},$$

and hence

$$19 \times_{27} 10 = 1.$$

Therefore $10^{-1} = 19$ in $\mathbb{Z}_{27}$.

A check: $19 \times 10 = 190 = 7 \times 27 + 1$, so $19 \times 10 \equiv 1 \pmod{27}$.

Exercise A97

Find the multiplicative inverse of

(a) 7 in $\mathbb{Z}_{16}$; (b) 8 in $\mathbb{Z}_{51}$.

The method demonstrated above can be used to find a multiplicative inverse of an element a in a number system $\mathbb{Z}_n$ whenever a and n are coprime. (The condition that a and n are coprime ensures that when we carry out backwards substitution we have 1 on the left-hand side of the equation; this 1 then becomes the 1 in the congruence of the form $ab \equiv 1 \pmod{n}$.)

On the other hand, if a and n are *not* coprime, then a has no multiplicative inverse in $\mathbb{Z}_n$. To see this, suppose that a and n are not coprime. If a did have a multiplicative inverse, say b, in $\mathbb{Z}_n$, then we would have

$$ab \equiv 1 \pmod{n},$$

that is,

$$ab = kn + 1 \text{ for some integer } k.$$

But a and n, not being coprime, are both divisible by some integer greater than 1, and hence $ab - kn$ is also divisible by this integer, which is impossible, since $ab - kn = 1$ by the equation above.

So we have the following result.

Theorem A11

Let n and a be positive integers, with a in $\mathbb{Z}_n$.

- If a and n are coprime, then a has a multiplicative inverse in $\mathbb{Z}_n$.
- If a and n are not coprime, then a does not have a multiplicative inverse in $\mathbb{Z}_n$.

Note that a more concise version of Theorem A11 is given in Subsection 1.4 of Unit A3, and this is the version stated in the module Handbook.

Theorem A11 gives us a further important result in the case when the modulus n is a *prime number*.

Remember that a **prime number** (or **prime**) is an integer greater than 1 whose only positive factors are 1 and itself; the first few primes are 2, 3, 5, 7, 11, 13, 17, and 19. In contrast, a **composite number** is an integer greater than 1 that is not a prime number; the first few composite numbers are 4, 6, 8, 9, 10, 12, 14, 15.

A prime number is necessarily coprime to every non-zero integer that is not a multiple of itself, so if p is a prime number, then every non-zero element of $\mathbb{Z}_p$ is coprime to p. Thus, by Theorem A11, we have the following result.

Multiplicative inverses in $\mathbb{Z}_p$

Let p be a prime number. Then every non-zero element in $\mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$.

It follows that for multiplication in $\mathbb{Z}_p$, where p is a prime, we can add the following property to the list of properties of multiplication in $\mathbb{Z}_n$.

M4 Multiplicative inverses For each non-zero $a \in \mathbb{Z}_p$ where p is a prime number, there is a number $a^{-1} \in \mathbb{Z}_p$ such that

$$a \times_p a^{-1} = 1 = a^{-1} \times_p a.$$

So arithmetic with $+_p$ and $\times_p$ in $\mathbb{Z}_p$, where p is a prime, satisfies all the properties A1–A5 and M1–M5; that is, for both addition and multiplication we have closure, associativity, an identity, inverses of all non-zero elements, and commutativity. Also, the distributive property (D1) holds for combining addition and multiplication. So, if p is a prime, then the number system $\mathbb{Z}_p$ with arithmetic modulo p satisfies all the properties in the list of eleven properties of $\mathbb{R}$ that you met in Subsection 1.2. It also satisfies the twelfth, trivial, property mentioned (since the additive identity 0 and multiplicative identity 1 of $\mathbb{Z}_p$ are not equal). Therefore, when p is a prime, the number system $\mathbb{Z}_p$ with arithmetic modulo p is a *field*, like $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$.

However, the multiplicative inverses property (M4) does not hold for $\mathbb{Z}_n$ if n is not prime, since in that case some elements $a \in \mathbb{Z}_n$ do not have multiplicative inverses. So in general the number system $\mathbb{Z}_n$ with arithmetic modulo n is *not* a field.

3.5 Solving linear equations in $\mathbb{Z}_n$

We now return to the question of whether we can find solutions of equations in modular arithmetic. We consider linear equations, that is, equations of the form

$$a \times_n x = b,$$

where $a, b \in \mathbb{Z}_n$. We seek all solutions $x \in \mathbb{Z}_n$.

Linear equations $a \times_n x = b$ where a and n are coprime

First we consider the case where a and n are coprime. In this case, by Theorem A11, a has a multiplicative inverse a^{-1}, and we can solve the linear equation above by multiplying both sides by this inverse. In the special case where n is a prime number, *every* element of $\mathbb{Z}_n$ has a multiplicative inverse, so every linear equation $a \times_n x = b$ has a solution.

Worked Exercise A42

Solve the equation $10 \times_{27} x = 14$.

Solution

In Worked Exercise A41 we found that the multiplicative inverse of 10 in $\mathbb{Z}_{27}$ is 19. Multiplying both sides of the given equation

$$10 \times_{27} x = 14$$

by this multiplicative inverse gives

$$10^{-1} \times_{27} 10 \times_{27} x = 10^{-1} \times_{27} 14,$$

that is,

$$1 \times_{27} x = 19 \times_{27} 14.$$

Since

$$19 \times 14 \equiv 266 \equiv 266 - 270 \equiv -4 \equiv 23 \pmod{27},$$

we have $x = 23$.

Hence the equation $10 \times_{27} x = 14$ has solution $x = 23$.

Note that the solution found in Worked Exercise A42 is the *only* solution of the given equation, because the multiplicative inverse of 10 in $\mathbb{Z}_{27}$ is unique.

In general, by an argument similar to that of Worked Exercise A42, if a and n are coprime, then the linear equation

$$a \times_n x = b$$

has the *unique* solution

$$x = a^{-1} \times_n b.$$

Exercise A98

Solve the following linear equations.

(a) $7 \times_{16} x = 3$ (b) $8 \times_{51} x = 19$

(By the solution to Exercise A97, we have $7^{-1} = 7$ in $\mathbb{Z}_{16}$, and $8^{-1} = 32$ in $\mathbb{Z}_{51}$.)

To use the method of Worked Exercise A42 to solve an equation $a \times_n x = b$ where a and n are coprime, we first need to find the multiplicative inverse in $\mathbb{Z}_n$ of the coefficient a of x. If we have not already found this inverse (for example, by using Euclid's Algorithm and backwards substitution), and the modulus n is fairly small, then the quickest way to solve the equation may be just to try different values of x. We know that there is a unique solution, so we can stop trying values once we have found a solution. Sometimes a solution can be spotted by using congruences, as in the following worked exercise.

Worked Exercise A43

Solve the equation $5 \times_{12} x = 7$.

Solution

Spotting a congruence for 7 (mod 12) that is a multiple of 5 can be helpful.

Observe that $7 \equiv -5 \pmod{12}$, and we know $5 \times (-1) = -5$, so we have

$$5 \times (-1) \equiv 7 \pmod{12}.$$

The integer -1 is not an element of $\mathbb{Z}_{12}$, but $-1 \equiv 11 \pmod{12}$, so

$$5 \times 11 \equiv 7 \pmod{12};$$

that is,

$$5 \times_{12} 11 = 7.$$

Hence the solution of the given equation is $x = 11$.

Exercise A99

Solve the following equations.

(a) $5 \times_{13} x = 2$ (b) $3 \times_{11} x = 5$

You may spot solutions using congruences as in Worked Exercise A43, or you may prefer to try values, or find and use multiplicative inverses.

Linear equations $a \times_n x = b$ where a and n are not coprime

Recall that we are considering the question of whether we can find solutions in $\mathbb{Z}_n$ of equations of the form

$$a \times_n x = b \qquad (5)$$

where $a, b \in \mathbb{Z}_n$. You have seen how to solve an equation of this form when a and n are coprime, so we now consider the case where a and n are not coprime.

In this case, the equation may not have any solutions. To see this, observe that if equation (5) *does* have a solution, say c, then

$$a \times_n c = b,$$

so

$$ac = b + kn \text{ for some integer } k,$$

which gives

$$b = ac - kn.$$

This equation tells us that any integer that is a factor of both a and n must also be a factor of b. Therefore, if equation (5) *does not* satisfy this condition – that is, if there is an integer that is a factor of both a and n but not a factor of b – then the equation has no solutions. In particular, if the highest common factor (HCF) of a and n is not a factor of b, then the equation has no solutions.

For example, the equation

$$6 \times_{18} x = 4$$

has no solutions, because the HCF of 6 and 18 is 3, and 3 is not a factor of 4.

On the other hand, if the HCF of a and n *is* a factor of b, then it turns out that the equation always has a solution; in fact, it has d solutions, where d is the HCF.

The box below summarises these facts about when the equation has solutions, and it also specifies what the solutions are when they exist.

Linear equations in $\mathbb{Z}_n$

Let d be the highest common factor of the integers a and n in the equation

$$a \times_n x = b.$$

- If d is not a factor of b, then the equation has no solutions in $\mathbb{Z}_n$.

- If d is a factor of b, then the equation has d solutions in $\mathbb{Z}_n$. These solutions are given by

$$x = c, \quad x = c + \frac{n}{d}, \quad x = c + \frac{2n}{d}, \quad \ldots, \quad x = c + \frac{(d-1)n}{d},$$

where c is the solution in $\mathbb{Z}_{n/d}$ of the simpler equation

$$\frac{a}{d} \times_{\frac{n}{d}} x = \frac{b}{d}.$$

(Since a/d and n/d are coprime, the simpler equation has a unique solution, which can be found using the methods given earlier.)

You will see a proof of the second bulleted statement in the box shortly. First, here is a worked exercise that illustrates the results in the box, and one similar exercise for you to try.

Worked Exercise A44

Solve the following equations.

(a) $4 \times_{12} x = 6$ (b) $6 \times_{15} x = 9$

Solution

(a) The HCF of 4 and 12 is 4, but this is not a factor of 6, so the equation $4 \times_{12} x = 6$ has no solutions.

(b) The HCF of 6 and 15 is $d = 3$, and this is also a factor of 9, so the equation $6 \times_{15} x = 9$ has $d = 3$ solutions.

To find these solutions, we start by finding the solution of the simpler equation

$$\frac{6}{3} \times_{\frac{15}{3}} x = \frac{9}{3},$$

that is,

$$2 \times_5 x = 3.$$

By trying possibilities, we find that the solution of this equation is

$$x = 4.$$

Also, $15/3 = 5$, so the solutions of the original equation are

$$x = 4, \quad x = 4 + 5 = 9, \quad x = x + 2 \times 5 = 14.$$

A quick check:

$$6 \times 4 = 24 \equiv 9 \pmod{15},$$
$$6 \times 9 = 54 \equiv 54 - 45 \equiv 9 \pmod{15},$$
$$6 \times 14 \equiv 6 \times (-1) \equiv -6 \equiv 9 \pmod{15},$$

as expected.

Exercise A100

Find all the solutions of the following equations.

(a) $9 \times_{12} x = 6$ (b) $8 \times_{12} x = 7$ (c) $5 \times_{12} x = 2$

(d) $4 \times_{16} x = 12$ (e) $3 \times_{16} x = 13$ (f) $8 \times_{16} x = 2$

As promised, here is a proof of the second bulleted statement in the box 'Linear equations in $\mathbb{Z}_n$'. Before reading it, look back to remind yourself what this statement says. To see why it holds, let c be the solution of the simpler equation, as stated. Then

$$\frac{a}{d} \times_{\frac{n}{d}} c = \frac{b}{d},$$

so

$$\frac{a}{d} c = \frac{b}{d} + k\frac{n}{d}$$

for some integer k, and hence (by multiplying throughout by d),

$$ac = b + kn,$$

so

$$a \times_n c = b,$$

that is, c is also a solution of the original equation.

Now consider all the integers r such that $c + r$ is in $\mathbb{Z}_n$ (where c is the solution discussed above). Let us consider the question: for which of these values of r is $c + r$ a solution of the original equation?

Well, saying that $c + r$ is a solution of the original equation is equivalent to saying that

$$a \times_n (c + r) = b,$$

which, by the multiplication property of congruences, is equivalent to saying that

$$a \times_n (c +_n r) = b.$$

By the distributive property for $+_n$ and $\times_n$, the equation above is equivalent to

$$(a \times_n c) +_n (a \times_n r) = b.$$

Now $a \times_n c = b$ (since c is a solution of the original equation), so the equation above is equivalent to

$$b +_n (a \times_n r) = b,$$

that is,

$$a \times_n r = 0.$$

So the values of r such that $c + r$ is a solution of the original equation are the values of r such that

ar is a multiple of n,

or, equivalently, since both a/d and n/d are integers,

$$\frac{a}{d}r \text{ is a multiple of } \frac{n}{d}.$$

Now we know that a/d is not a multiple of n/d, since these two integers are coprime, so the statement above holds precisely when r is a multiple of n/d. So our conclusion is that the element $c + r$ of $\mathbb{Z}_n$ is a solution of the original equation precisely when r is a multiple of n/d. This is what the second bulleted point in the box claims. (Note that the next multiple of n/d after $(d-1)n/d$ is $dn/d = n$, and adding n to c gives a number that is too large to be in $\mathbb{Z}_n$.)

Summary

In this unit you have studied the properties of various different number systems. You have seen that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ (for p prime) all satisfy the eleven standard arithmetical properties you met in Subsection 1.2 (together with the trivial twelfth property) and so are all *fields*, and that the existence of a multiplicative inverse for every non-zero element means that every linear equation in these number systems has a solution. You also saw that in number systems that are not fields, for example, in $\mathbb{Z}$ and in $\mathbb{Z}_n$, where n is not prime, some, but certainly not all, linear equations have solutions. In the field $\mathbb{C}$, you saw that every *polynomial* equation with complex coefficients has a solution, and explored ways of finding such a solution in certain special cases.

These number systems and their properties are used throughout the rest of the module.

Learning outcomes

After working through this unit, you should be able to:

- understand the arithmetic properties of the rational and real numbers
- understand the properties a number system satisfies if it is a *field*
- understand and use the Factor Theorem
- understand the definition of a *complex number* and represent complex numbers as points in the *complex plane*
- perform arithmetic operations with complex numbers in *Cartesian*, *polar* and *exponential form*, and convert between these forms as appropriate
- use de Moivre's Theorem to find the nth roots of a complex number
- understand the Division Theorem and the properties of *congruences*, and perform *modular arithmetic*
- use Euclid's Algorithm and backwards substitution to find multiplicative inverses in modular arithmetic, where these exist
- solve linear equations in $\mathbb{Z}_n$.

Solutions to exercises

Solution to Exercise A57

(a) There is no integer 2^{-1} such that $2 \times 2^{-1} = 2^{-1} \times 2 = 1$, since $\frac{1}{2} \notin \mathbb{Z}$, for example.

(b) Only the numbers 1 and -1 have a multiplicative inverse in $\mathbb{Z}$. (The multiplicative inverse of 1 is 1, and of -1 is -1.)

Solution to Exercise A58

(a) **(i)** The equation has solution $x = -2$, which belongs to $\mathbb{Q}$.

(ii) The equation has solution $x = -\frac{1}{5}$, which belongs to $\mathbb{Q}$.

(b) **(i)** The equation has solution $x = 3$, which belongs to $\mathbb{R}$.

(ii) The equation has solution $x = -\dfrac{7}{\sqrt{3}}$, which belongs to $\mathbb{R}$.

Solution to Exercise A59

(a) Factorising the equation

$$x^2 - 7x + 12 = 0$$

gives

$$(x-3)(x-4) = 0.$$

So this equation has two solutions in $\mathbb{R}$, namely $x = 3$ and $x = 4$.

(b) Factorising the equation

$$x^2 + 6x + 9 = 0$$

gives

$$(x+3)^2 = 0.$$

So this equation has one solution in $\mathbb{R}$, namely $x = -3$.

(c) Factorising the equation

$$2x^2 + 5x - 3 = 0$$

gives

$$(2x-1)(x+3) = 0.$$

So this equation has two solutions in $\mathbb{R}$, namely $x = \frac{1}{2}$ and $x = -3$.

(d) Applying the quadratic formula to the equation

$$2x^2 - 2x - 1 = 0$$

gives

$$x = \frac{2 \pm \sqrt{4+8}}{4} = \frac{1}{2} \pm \frac{1}{2}\sqrt{3}.$$

This equation has two solutions in $\mathbb{R}$.

(e) Applying the quadratic formula to the equation

$$x^2 - 2x + 5 = 0$$

gives

$$x = \frac{2 \pm \sqrt{4-20}}{2}.$$

Since $4 - 20 = -16$, which is negative, this equation has no solutions in $\mathbb{R}$.

(f) Factorising the equation

$$x^2 - 2\sqrt{3}x + 3 = 0$$

gives

$$\left(x - \sqrt{3}\right)^2 = 0.$$

So this equation has one solution in $\mathbb{R}$, namely $x = \sqrt{3}$.

Solution to Exercise A60

(a) By the Factor Theorem (Theorem A2), $x + 3$ is a factor of $p(x)$ if and only if $p(-3) = 0$, that is,

$$\begin{aligned} 0 &= (-3)^3 + k(-3)^2 + 6(-3) + 36 \\ &= -27 + 9k - 18 + 36 \\ &= 9k - 9. \end{aligned}$$

This equation has just one solution, $k = 1$, so the only value of k for which $x + 3$ is a factor of $p(x)$ is $k = 1$.

(b) We have

$$x^3 + x^2 + 6x + 36 = (x+3)(ax^2 + bx + c),$$

for some real numbers a, b and c.

Equating the coefficients of x^3 gives $1 = a$. Comparing the constant terms gives $36 = 3c$, so $c = 12$. Thus we have

$$x^3 + x^2 + 6x + 36 = (x+3)(x^2 + bx + 12).$$

Equating the coefficients of x^2 gives $1 = 3 + b$, so $b = -2$. Hence

$$x^3 + x^2 + 6x + 36 = (x+3)(x^2 - 2x + 12).$$

Solution to Exercise A61

(a) Since all the roots are integers, the only possible roots are the factors of -15, that is, $\pm1, \pm3, \pm5, \pm15$. Considering these in turn, we obtain the following table.

x	1	-1	3	-3	5	$\cdots$
$p(x)$	0	-48	0	-192	0	$\cdots$

We do not need to work out any more values, as we already have three roots: $x = 1$, $x = 3$ and $x = 5$. So, since the coefficient of x^3 is 1,

$$p(x) = (x-1)(x-3)(x-5).$$

As a check, we note that the coefficient of x^2 is equal to minus the sum of the roots, $-9 = -(1 + 3 + 5)$.

(b) Let

$$p(x) = x^3 - 3x^2 + 4.$$

Since all the roots of $p(x)$ are integers, the only possible roots are the factors of 4, that is, $\pm1, \pm2, \pm4$. Considering these in turn, we obtain the following table.

x	1	-1	2	-2	4	-4
$p(x)$	2	0	0	-16	20	-108

Thus the only solutions are $x = -1$ and $x = 2$. Since $p(x)$ is a cubic polynomial, it must have three linear factors, so one of these solutions must give rise to a repeated factor. The coefficient of x^2 is -3, and this must equal minus the sum of the roots. This is only possible if $(x-2)$ is the repeated factor; we then have $-3 = -(2 + 2 - 1)$. The coefficient of x^3 is 1, so

$$p(x) = (x-2)(x-2)(x+1).$$

Solution to Exercise A62

(a) A suitable equation is

$$(x-1)(x-2)(x-3)(x+3) = 0,$$

that is,

$$x^4 - 3x^3 - 7x^2 + 27x - 18 = 0.$$

There are many other possibilities; for example, any of the factors could be repeated.

(b) A suitable equation is

$$(x-2)(x-2)(x-3) = 0,$$

that is,

$$x^3 - 7x^2 + 16x - 12 = 0.$$

Another possibility is

$$(x-2)(x-3)(x-3) = 0,$$

that is,

$$x^3 - 8x^2 + 21x - 18 = 0.$$

Solution to Exercise A63

(a) The equation $z^2 - 4z + 7 = 0$ has solutions

$$\begin{aligned} z = \frac{4 \pm \sqrt{16-28}}{2} &= \frac{4 \pm \sqrt{-12}}{2} \\ &= 2 \pm \frac{i\sqrt{12}}{2} \\ &= 2 \pm i\sqrt{3}; \end{aligned}$$

that is, the solutions are $z = 2 + i\sqrt{3}$ and $z = 2 - i\sqrt{3}$.

(b) The equation $z^2 - iz + 2 = 0$ has solutions

$$\begin{aligned} z = \frac{i \pm \sqrt{i^2 - 8}}{2} &= \frac{i}{2} \pm \frac{\sqrt{-9}}{2} \\ &= \frac{i}{2} \pm \frac{3i}{2}; \end{aligned}$$

that is, the solutions are $z = 2i$ and $z = -i$.

(c) We can factorise the equation

$$z^3 - 3z^2 + 4z - 2 = 0$$

as

$$(z-1)(az^2 + bz + c) = 0,$$

and by equating coefficients we have $a = 1$, $c = 2$ and $b = -2$ giving

$$(z-1)(z^2 - 2z + 2) = 0.$$

Hence $z = 1$ or

$$\begin{aligned} z &= \frac{2 \pm \sqrt{4-8}}{2} \\ &= \frac{2 \pm 2\sqrt{-1}}{2} \\ &= 1 \pm i, \end{aligned}$$

so the solutions are $z = 1$, $z = 1 + i$ and $z = 1 - i$.

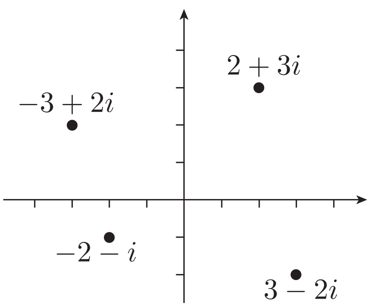
(d) The equation $z^4 - 16 = 0$ can be factorised as

$$(z^2 - 4)(z^2 + 4) = 0$$

giving $z^2 = 4$ or $z^2 = -4$, so $z = \pm 2$ or $z = \pm 2i$.

Hence the solutions are $z = 2$, $z = -2$, $z = 2i$ and $z = -2i$.

Solution to Exercise A64



Solution to Exercise A65

(a) $(3 - 5i) + (2 + 4i) = 5 - i$

(b) $$\begin{aligned} (2-3i)(-3+2i) &= -6 + 9i + 4i - 6i^2 \\ &= 13i \end{aligned}$$

(c) $$\begin{aligned} (5+3i)^2 &= (5+3i)(5+3i) \\ &= 25 + 15i + 15i + 9i^2 \\ &= 16 + 30i \end{aligned}$$

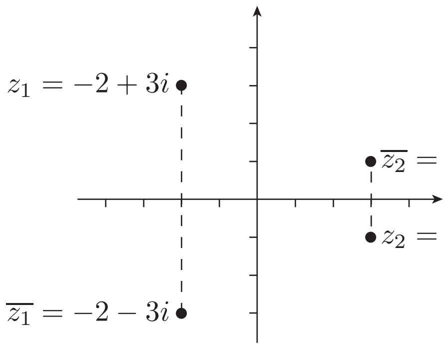
(d) $$\begin{aligned} (1+i)(7+2i) &= 7 + 7i + 2i + 2i^2 \\ &= 5 + 9i, \end{aligned}$$

so

$$\begin{aligned} (1+i)(7+2i)(4-i) &= (5+9i)(4-i) \\ &= 20 + 36i - 5i - 9i^2 \\ &= 29 + 31i. \end{aligned}$$

Solution to Exercise A66

$\overline{z_1} = -2 - 3i$ and $\overline{z_2} = 3 + i$.



Solution to Exercise A67

Property 2

Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$. Then

$$\begin{aligned} z_1 z_2 &= (x_1 + iy_1)(x_2 + iy_2) \\ &= x_1x_2 + ix_2y_1 + ix_1y_2 + i^2y_1y_2 \\ &= (x_1x_2 - y_1y_2) + i(x_2y_1 + x_1y_2), \end{aligned}$$

so

$$\overline{z_1 z_2} = (x_1x_2 - y_1y_2) - i(x_2y_1 + x_1y_2).$$

Also,

$$\begin{aligned} \overline{z_1} \times \overline{z_2} &= (x_1 - iy_1)(x_2 - iy_2) \\ &= x_1x_2 - ix_2y_1 - ix_1y_2 + i^2y_1y_2 \\ &= (x_1x_2 - y_1y_2) - i(x_2y_1 + x_1y_2). \end{aligned}$$

Therefore

$$\overline{z_1 z_2} = \overline{z_1} \times \overline{z_2}.$$

Property 3

Let $z = x + iy$. Then

$$\begin{aligned} z + \overline{z} &= x + iy + x - iy \\ &= 2x \\ &= 2\,\mathrm{Re}\,z. \end{aligned}$$

Property 4 Let $z = x + iy$. Then

$$\begin{aligned} z - \overline{z} &= x + iy - (x - iy) \\ &= 2iy \\ &= 2i \operatorname{Im} z. \end{aligned}$$

Solution to Exercise A68

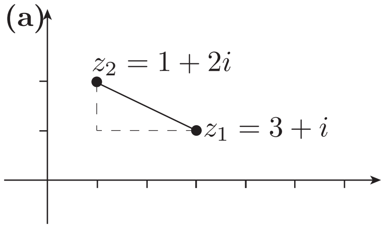
(a) $\begin{aligned}[t] |5 + 12i| &= \sqrt{5^2 + 12^2} \\ &= \sqrt{169} = 13 \end{aligned}$

(b) $|1 + i| = \sqrt{1^2 + 1^2} = \sqrt{2}$

(c) $|-5| = \sqrt{(-5)^2 + 0^2} = 5$

Solution to Exercise A69

(a)



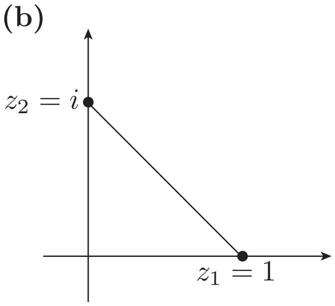
Here

$$z_1 - z_2 = (3 + i) - (1 + 2i) = 2 - i,$$

so

$$|z_1 - z_2| = \sqrt{2^2 + (-1)^2} = \sqrt{5}.$$

(b)



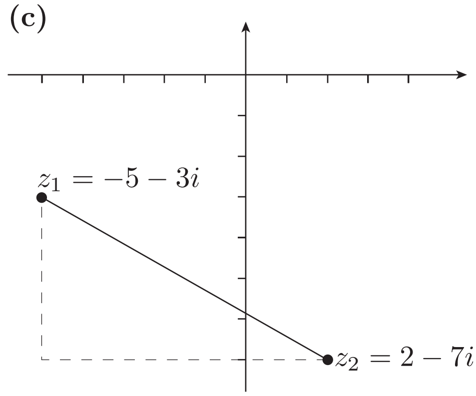
Here

$$z_1 - z_2 = 1 - i,$$

so

$$|z_1 - z_2| = \sqrt{1^2 + (-1)^2} = \sqrt{2}.$$

(c)



Here

$$z_1 - z_2 = (-5 - 3i) - (2 - 7i) = -7 + 4i,$$

so

$$|z_1 - z_2| = \sqrt{(-7)^2 + 4^2} = \sqrt{65}.$$

Solution to Exercise A70

In each case we multiply both the numerator and the denominator by the complex conjugate of the denominator, and use $z\overline{z} = |z|^2$.

(a) $\begin{aligned}[t] \frac{1}{3 - i} &= \frac{3 + i}{(3 - i)(3 + i)} \\ &= \frac{3 + i}{3^2 + (-1)^2} \\ &= \tfrac{3}{10} + \tfrac{1}{10}i \\ &= \tfrac{1}{10}(3 + i) \end{aligned}$

(b) $\begin{aligned}[t] \frac{1}{-1 + 2i} &= \frac{-1 - 2i}{(-1 + 2i)(-1 - 2i)} \\ &= \frac{-1 - 2i}{(-1)^2 + 2^2} \\ &= -\tfrac{1}{5} - \tfrac{2}{5}i \\ &= -\tfrac{1}{5}(1 + 2i) \end{aligned}$

Solution to Exercise A71

In each case we multiply the numerator and denominator by the complex conjugate of the denominator, and use $z\overline{z} = |z|^2$.

(a) $\begin{aligned}[t] \frac{5}{2 - i} &= \frac{5(2 + i)}{(2 - i)(2 + i)} \\ &= \frac{10 + 5i}{2^2 + (-1)^2} \\ &= \tfrac{1}{5}(10 + 5i) \\ &= 2 + i \end{aligned}$

(b) $$\frac{2+3i}{-3+4i} = \frac{(2+3i)(-3-4i)}{(-3+4i)(-3-4i)}$$
$$= \frac{-6-9i-8i-12i^2}{(-3)^2+4^2}$$
$$= \frac{6-17i}{(-3)^2+4^2}$$
$$= \tfrac{6}{25} - \tfrac{17}{25}i$$
$$= \tfrac{1}{25}(6-17i)$$

Solution to Exercise A72

(a) The required form is $x+iy$, where

$$x = 2\cos\frac{\pi}{2} = 0$$

and

$$y = 2\sin\frac{\pi}{2} = 2.$$

The Cartesian form is therefore $2i$.

(b) The required form is $x+iy$, where

$$x = 4\cos\left(-\frac{2\pi}{3}\right) = 4\cos\frac{2\pi}{3}$$
$$= -4\cos\frac{\pi}{3} = -2$$

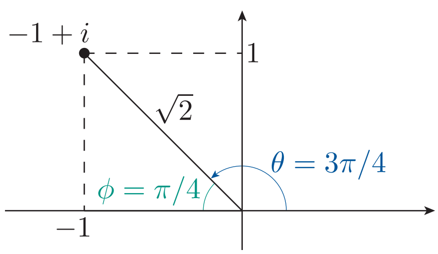
and

$$y = 4\sin\left(-\frac{2\pi}{3}\right) = -4\sin\frac{2\pi}{3}$$
$$= -4\sin\frac{\pi}{3} = -2\sqrt{3}.$$

The Cartesian form is therefore $-2(1+i\sqrt{3})$.

Solution to Exercise A73

(a) Let $z = x+iy = -1+i$, so $x=-1$ and $y=1$.



Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{(-1)^2+1^2} = \sqrt{2}.$$

Also

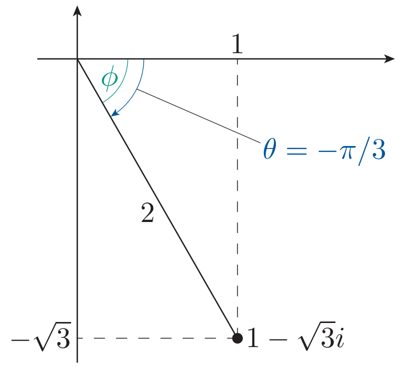
$$\cos\phi = \frac{|x|}{r} = \frac{1}{\sqrt{2}}.$$

So $\phi = \pi/4$, and from the diagram (or because z lies in the second quadrant) we have $\theta = \pi - \phi = 3\pi/4$.

Thus the polar form of $-1+i$ in terms of the principal argument is

$$\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right).$$

(b) Let $z = x+iy = 1-i\sqrt{3}$, so $x=1$ and $y=-\sqrt{3}$.



Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{1^2+(-\sqrt{3})^2} = 2.$$

Also

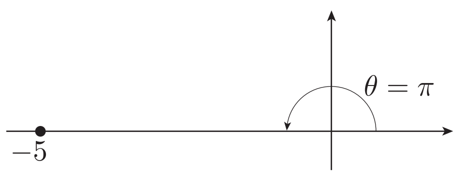
$$\cos\phi = \frac{|x|}{r} = \frac{1}{2}.$$

So $\phi = \pi/3$, and z lies in the fourth quadrant, so $\theta = -\phi = -\pi/3$.

Thus the polar form of $1-i\sqrt{3}$ in terms of the principal argument is

$$2\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right).$$

(c) Let $z = x+iy = -5$, so $x=-5$ and $y=0$.



Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{(-5)^2+0^2} = 5.$$

Also z lies on the negative half of the real axis, so $\theta = \pi$.

Thus the polar form of -5 in terms of the principal argument is

$$5(\cos\pi + i\sin\pi).$$

Solution to Exercise A74

(a) The modulus of the product is

$$4 \times \tfrac{1}{2} = 2.$$

An argument is

$$-\frac{\pi}{6} + \frac{7\pi}{8} = \frac{17\pi}{24}.$$

Since this argument lies in $(-\pi, \pi]$, it is the principal argument. The required product is therefore

$$2\left(\cos\frac{17\pi}{24} + i\sin\frac{17\pi}{24}\right).$$

The modulus of the quotient is

$$4 \div \tfrac{1}{2} = 8.$$

An argument is

$$-\frac{\pi}{6} - \frac{7\pi}{8} = -\frac{25\pi}{24}.$$

The principal argument is therefore

$$-\frac{25\pi}{24} + 2\pi = \frac{23\pi}{24}.$$

The required quotient is therefore

$$8\left(\cos\frac{23\pi}{24} + i\sin\frac{23\pi}{24}\right).$$

(b) The modulus of the product is

$$3 \times \tfrac{1}{2} = \tfrac{3}{2}.$$

An argument is

$$\frac{2\pi}{3} + \frac{\pi}{2} = \frac{7\pi}{6}.$$

The principal argument is therefore

$$\frac{7\pi}{6} - 2\pi = -\frac{5\pi}{6}.$$

The required product is therefore

$$\frac{3}{2}\left(\cos\left(-\frac{5\pi}{6}\right) + i\sin\left(-\frac{5\pi}{6}\right)\right).$$

The modulus of the quotient is

$$3 \div \tfrac{1}{2} = 6.$$

An argument is

$$\frac{2\pi}{3} - \frac{\pi}{2} = \frac{\pi}{6}.$$

Since this argument lies in $(-\pi, \pi]$, it is the principal argument. The required quotient is therefore

$$6\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right).$$

Solution to Exercise A75

From the solution to Exercise A73,

$$z_1 = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right),$$

$$z_2 = 2\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right),$$

$$z_3 = 5(\cos\pi + i\sin\pi).$$

Hence

$$\begin{aligned} z_1z_2z_3 &= 10\sqrt{2}\left(\cos\left(\frac{3\pi}{4} - \frac{\pi}{3} + \pi\right)\right. \\ &\qquad \left. + i\sin\left(\frac{3\pi}{4} - \frac{\pi}{3} + \pi\right)\right) \\ &= 10\sqrt{2}\left(\cos\frac{17\pi}{12} + i\sin\frac{17\pi}{12}\right) \\ &= 10\sqrt{2}\left(\cos\left(-\frac{7\pi}{12}\right) + i\sin\left(-\frac{7\pi}{12}\right)\right), \end{aligned}$$

using the principal argument.

Also

$$\begin{aligned} \frac{z_2z_3}{z_1} &= \frac{10}{\sqrt{2}}\left(\cos\left(-\frac{\pi}{3} + \pi - \frac{3\pi}{4}\right)\right. \\ &\qquad \left. + i\sin\left(-\frac{\pi}{3} + \pi - \frac{3\pi}{4}\right)\right) \\ &= 5\sqrt{2}\left(\cos\left(-\frac{\pi}{12}\right) + i\sin\left(-\frac{\pi}{12}\right)\right). \end{aligned}$$

Solution to Exercise A76

(a) $1 = \cos 0 + i \sin 0$

(b) If $z_0 = \cos 0 + i\sin 0$, then, by de Moivre's Theorem,

$$z_0^3 = \cos 0 + i \sin 0 = 1.$$

If $z_1 = \cos(2\pi/3) + i\sin(2\pi/3)$, then, by de Moivre's Theorem,

$$\begin{aligned} z_1^3 &= \cos 2\pi + i \sin 2\pi \\ &= \cos 0 + i \sin 0 = 1. \end{aligned}$$

If $z_2 = \cos(4\pi/3) + i\sin(4\pi/3)$, then, by de Moivre's Theorem,

$$\begin{aligned} z_2^3 &= \cos 4\pi + i \sin 4\pi \\ &= \cos 0 + i \sin 0 = 1. \end{aligned}$$

(c) In Cartesian form,

$$\begin{aligned} z_0 &= 1, \\ z_1 &= -\frac{1}{2}\left(1 - i\sqrt{3}\right), \\ z_2 &= -\frac{1}{2}\left(1 + i\sqrt{3}\right). \end{aligned}$$

Solution to Exercise A77

(a) Let $z = r(\cos\theta + i \sin\theta)$. Then, since

$$1 = 1(\cos 0 + i \sin 0),$$

we have

$$\begin{aligned} z^6 &= r^6(\cos 6\theta + i \sin 6\theta) \\ &= 1(\cos 0 + i \sin 0). \end{aligned}$$

Hence $r = 1^{1/6} = 1$ and $\theta = 0 + \dfrac{2k\pi}{6}$ for $k = 0, 1, \ldots, 5$, and the six solutions of $z^6 = 1$ are given by

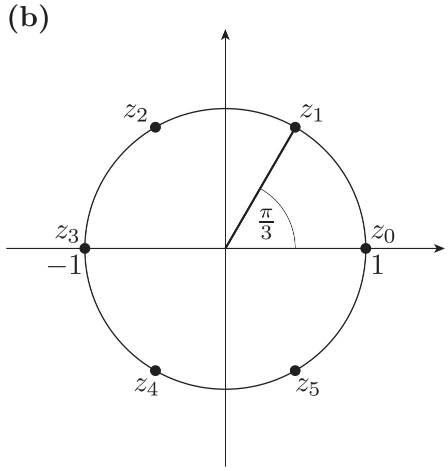
$$z = \cos\frac{2k\pi}{6} + i \sin\frac{2k\pi}{6}$$

for $k = 0, 1, \ldots, 5$.

Hence the solutions using the principal arguments are

$$\begin{aligned} z_0 &= \cos 0 + i \sin 0, \\ z_1 &= \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}, \\ z_2 &= \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}, \\ z_3 &= \cos\pi + i\sin\pi, \\ z_4 &= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} \\ &= \cos\left(-\frac{2\pi}{3}\right) + i\sin\left(-\frac{2\pi}{3}\right), \\ z_5 &= \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3} \\ &= \cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right). \end{aligned}$$

(b)



(c) $z_0 = 1,$
$z_1 = \frac{1}{2}(1 + i\sqrt{3}),$
$z_2 = -\frac{1}{2}(1 - i\sqrt{3}),$
$z_3 = -1,$
$z_4 = -\frac{1}{2}(1 + i\sqrt{3}),$
$z_5 = \frac{1}{2}(1 - i\sqrt{3}).$

Solution to Exercise A78

Let $z = r(\cos\theta + i\sin\theta)$. Then, since

$$-4 = 4(\cos\pi + i\sin\pi),$$

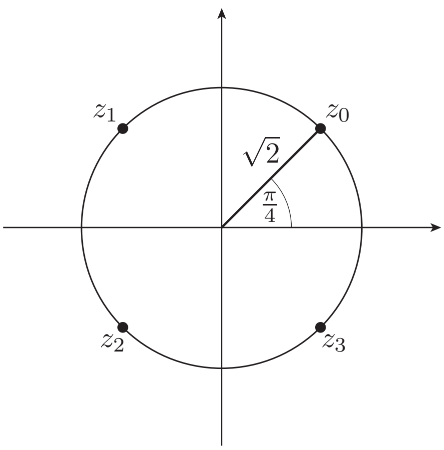
we have

$$z^4 = r^4(\cos 4\theta + i\sin 4\theta) = 4(\cos\pi + i\sin\pi).$$

Hence $r = 4^{1/4} = \sqrt{2}$ and $\theta = \dfrac{\pi}{4} + \dfrac{2k\pi}{4}$ for $k = 0, 1, 2, 3$.

So the solutions are

$$\begin{aligned} z_0 &= \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = 1 + i,\\ z_1 &= \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right) = -1 + i,\\ z_2 &= \sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right) = -1 - i,\\ z_3 &= \sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right) = 1 - i. \end{aligned}$$



Solution to Exercise A79

Let $z = r(\cos\theta + i\sin\theta)$.

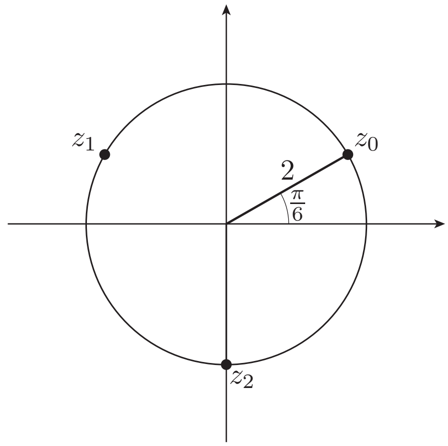
Since $8i = 8\left(\cos\dfrac{\pi}{2} + i\sin\dfrac{\pi}{2}\right)$, we have

$$\begin{aligned} z^3 &= r^3(\cos 3\theta + i\sin 3\theta)\\ &= 8\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right). \end{aligned}$$

Hence $r = 8^{1/3} = 2$ and $\theta = \dfrac{\pi}{6} + \dfrac{2k\pi}{3}$ for $k = 0, 1, 2$.

So the solutions are

$$\begin{aligned} z_0 &= 2\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right) = \sqrt{3} + i,\\ z_1 &= 2\left(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}\right) = -\sqrt{3} + i,\\ z_2 &= 2\left(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}\right) = -2i. \end{aligned}$$



Solution to Exercise A80

(a) We have

$$\begin{aligned} p(2i) &= (2i)^4 - 2(2i)^3 + 7(2i)^2 - 8(2i) + 12\\ &= 16i^4 - 16i^3 + 28i^2 - 16i + 12\\ &= 16 + 16i - 28 - 16i + 12\\ &= 0, \end{aligned}$$

so $2i$ is a root of $p(z)$.

(b) Since p has real coefficients, $z = -2i$ is also a root of $p(z)$, so $(z - 2i)(z + 2i) = z^2 + 4$ is a factor of $p(z)$.

By equating coefficients, we obtain
$z^4 - 2z^3 + 7z^2 - 8z + 12 = (z^2 + 4)(z^2 - 2z + 3)$.

So the remaining two roots of $p(z)$ are the solutions of the equation $z^2 - 2z + 3 = 0$.

Using the quadratic formula, we have

$$\begin{aligned} z &= \frac{2 \pm \sqrt{4 - 12}}{2}\\ &= \frac{2 \pm \sqrt{-8}}{2}\\ &= \frac{2 \pm 2\sqrt{-2}}{2}\\ &= 1 \pm i\sqrt{2}. \end{aligned}$$

Hence the four roots of $p(z)$ are $2i$, $-2i$, $1+i\sqrt{2}$ and $1-i\sqrt{2}$.

Solution to Exercise A81

A suitable polynomial is

$$(z-1)(z+2)(z-3i)(z+3i),$$

that is,

$$(z^2+z-2)(z^2+9)$$

or

$$z^4+z^3+7z^2+9z-18.$$

Solution to Exercise A82

(a) Let $z=x+iy$; then

$$\begin{aligned}\frac{1}{e^z} &= \frac{1}{e^{x+iy}}\\ &= \frac{1}{e^x(\cos y+i\sin y)} \quad \text{(by definition)}\\ &= e^{-x}(\cos y+i\sin y)^{-1}\\ &= e^{-x}(\cos(-y)+i\sin(-y))\end{aligned}$$

(by de Moivre's Theorem with $n=-1$)

$$\begin{aligned} &= e^{-x+i(-y)} \quad \text{(by definition)}\\ &= e^{-z}.\end{aligned}$$

(b) $$\begin{aligned}\frac{e^{z_1}}{e^{z_2}} &= e^{z_1}\times\frac{1}{e^{z_2}}\\ &= e^{z_1}e^{-z_2} \quad \text{(by part (a))}\\ &= e^{z_1+(-z_2)} \quad \text{(by Worked Exercise A36)}\\ &= e^{z_1-z_2}.\end{aligned}$$

Solution to Exercise A83

Euler's Identity is $e^{i\pi}+1=0$; that is, $-1=e^{i\pi}$.

We have

$$\begin{aligned}-z &= -1\times re^{i\theta}\\ &= e^{i\pi}\times re^{i\theta} \quad \text{(by Euler's Identity)}\\ &= re^{i(\theta+\pi)}.\end{aligned}$$

Solution to Exercise A84

(a) $65=9\times 7+2$, so the quotient is 9 and the remainder is 2.

(b) $-256=-20\times 13+4$, so the quotient is -20 and the remainder is 4.

Solution to Exercise A85

(a) The possible remainders are 0, 1, 2, 3, 4, 5 and 6.

(b) There are many possible answers here; for example, 3, 10, -4 and -11.

Solution to Exercise A86

We have

$$\begin{aligned}25 &\equiv 8 \pmod{17},\\ 53 &\equiv 2 \pmod{17},\\ -15 &\equiv 2 \pmod{17},\\ 3 &\equiv 3 \pmod{17},\\ 127 &\equiv 8 \pmod{17},\end{aligned}$$

so the remainders are 8, 2, 2, 3 and 8, respectively. So $25\equiv 127 \pmod{17}$ and $53\equiv -15 \pmod{17}$.

Solution to Exercise A87

Suppose that $a\equiv b \pmod{n}$ and $c\equiv d \pmod{n}$. Then $a-b=kn$ and $c-d=ln$ for some integers k and l. Hence $a=b+kn$ and $c=d+ln$ for some integers k and l, so

$$\begin{aligned}ac &= (b+kn)(d+ln)\\ &= bd+bln+knd+kln^2\\ &= bd+n(bl+kd+kln).\end{aligned}$$

Therefore $ac-bd=(bl+kd+kln)n$. Since $bl+kd+kln$ is an integer, it follows that $ac\equiv bd \pmod{n}$. Thus the multiplication property holds.

Solution to Exercise A88

(a) Using the transitivity property of congruences we obtain

$$3869\equiv 669\equiv 29\equiv 13 \pmod{16}$$

and

$$1685\equiv 85\equiv 5 \pmod{16},$$

so 3869 has remainder 13 on division by 16, and 1685 has remainder 5 on division by 16.

(b) Using the addition property of congruences and the answer to part (a), we obtain

$$(3869 + 1685) \equiv (13 + 5) \equiv 18 \equiv 2 \pmod{16},$$

so $3869 + 1685$ has remainder 2 on division by 16.

(c) Using the powers property of congruences and the answer to part (b), we obtain

$$(3869 + 1685)^4 \equiv 2^4 \equiv 16 \equiv 0 \pmod{16},$$

so $(3869 + 1685)^4$ has remainder 0 on division by 16; that is, $(3869 + 1685)^4$ is divisible by 16.

Since

$$\begin{aligned}&(3869 + 1685)^{111}\\ &\quad = (3869 + 1685)^4 \times (3869 + 1685)^{107},\end{aligned}$$

the multiplication property of congruences gives

$$\begin{aligned}(3869 + 1685)^{111} &\equiv 0 \times (3869 + 1685)^{107}\\ &\equiv 0 \pmod{16}.\end{aligned}$$

Hence $(3869 + 1685)^{111}$ has remainder 0 on division by 16; that is, it is divisible by 16.

Alternatively, it is possible to conclude directly that $(3869 + 1685)^{111}$ is divisible by 16 (and hence has remainder 0 on division by 16) since it is divisible by $(3869 + 1685)^4$.

Solution to Exercise A89

(a) $3 +_5 2 = 0$

(b) $4 +_{17} 5 = 9$

(c) $8 +_{16} 12 = 4$

(d) $3 \times_5 2 = 1$

(e) $4 \times_{17} 5 = 3$

(f) $8 \times_{16} 12 = 0$

Solution to Exercise A90

There are many ways to calculate these products in modular arithmetic; your method may differ from those below.

(a) We have

$$\begin{aligned}7 \times 26 &\equiv 7 \times (-1)\\ &\equiv -7\\ &\equiv 20 \pmod{27}.\end{aligned}$$

Thus $7 \times_{27} 26 = 20$.

(b) We have

$$\begin{aligned}16 \times 14 &\equiv 8 \times 2 \times 14\\ &\equiv 8 \times 28\\ &\equiv 8 \times (-1)\\ &\equiv -8\\ &\equiv 21 \pmod{29}.\end{aligned}$$

Thus $16 \times_{29} 14 = 21$.

(c) We have

$$\begin{aligned}9 \times 15 &\equiv 3 \times 3 \times 15\\ &\equiv 3 \times 45\\ &\equiv 3 \times 12\\ &\equiv 36\\ &\equiv 3 \pmod{33}.\end{aligned}$$

Thus $9 \times_{33} 15 = 3$.

(d) We have

$$\begin{aligned}37 \times 23 &\equiv -8 \times 23\\ &\equiv -4 \times 2 \times 23\\ &\equiv -4 \times 46\\ &\equiv -4 \times 1\\ &\equiv -4\\ &\equiv 41 \pmod{45}.\end{aligned}$$

Thus $37 \times_{45} 23 = 41$.

(e) We have

$$\begin{aligned}15 \times 6 &\equiv 15 \times 2 \times 3\\ &\equiv 30 \times 3\\ &\equiv -4 \times 3\\ &\equiv -12\\ &\equiv 22 \pmod{34}.\end{aligned}$$

Thus $15 \times_{34} 6 = 22$.

(f) We have

$$\begin{aligned}9 \times 18 &\equiv 9 \times 9 \times 2\\ &\equiv 81 \times 2\\ &\equiv 1 \times 2\\ &\equiv 2 \pmod{40}.\end{aligned}$$

Thus $9 \times_{40} 18 = 2$.

Solution to Exercise A91

(a) From the tables, we have the following.

(i) $3 +_4 3 = 2$, so if $x +_4 3 = 2$ then $x = 3$.

(ii) $4 +_7 5 = 2$, so if $x +_7 5 = 2$ then $x = 4$.

(iii) $2 +_4 2 = 0$, so if $x +_4 2 = 0$ then $x = 2$.

(iv) $2 +_7 5 = 0$, so if $x +_7 5 = 0$ then $x = 2$.

(b) You may have noticed that:

- each element appears exactly once in each row and exactly once in each column
- there is a pattern of diagonal stripes of unique numbers running down from right to left.

Solution to Exercise A92

(a)

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) $x +_6 1 = 5$ has solution $x = 4$.

$x +_6 5 = 1$ has solution $x = 2$.

Solution to Exercise A93

By definition, $a +_n b$ and $b +_n a$ are the remainders of the integers $a + b$ and $b + a$, respectively, on division by n. Since ordinary addition is commutative, we have $a + b = b + a$, so $a +_n b = b +_n a$, and the commutative property (A5) holds.

Solution to Exercise A94

(a)

a	0	1	2	3	4	5	6
$-_7 a$	0	6	5	4	3	2	1

(b)

a	0	1	2	$\dots$	r	$\dots$	$n-1$
$-_n a$	0	$n-1$	$n-2$	$\dots$	$n-r$	$\dots$	1

The additive inverse of 0 is always 0, since $0 +_n 0 = 0$.

For any integer $r > 0$ in $\mathbb{Z}_n$, $n - r \in \mathbb{Z}_n$ and $r + (n - r) = n$, so $r +_n (n - r) = 0$.

Solution to Exercise A95

(a) (i) The elements 1 and 3 of $\mathbb{Z}_4$ have multiplicative inverses in $\mathbb{Z}_4$: 1 has multiplicative inverse 1 since $1 \times_4 1 = 1$, and similarly 3 has multiplicative inverse 3 since $3 \times_4 3 = 1$. The other elements of $\mathbb{Z}_4$, namely 0 and 2, do not have multiplicative inverses.

(ii) The non-zero elements of $\mathbb{Z}_7$ have multiplicative inverses as given in the following table, where b is a multiplicative inverse of a.

a	1	2	3	4	5	6
b	1	4	5	2	3	6

(b)

$\times_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

The elements 1, 3, 7 and 9 of $\mathbb{Z}_{10}$ have multiplicative inverses in $\mathbb{Z}_{10}$, as given in the following table, where b is a multiplicative inverse of a.

a	1	3	7	9
b	1	7	3	9

The other elements of $\mathbb{Z}_{10}$, namely 0, 2, 4, 5, 6 and 8, do not have multiplicative inverses.

Solution to Exercise A96

Applying Euclid's Algorithm gives

$$\begin{aligned} 201 &= 2 \times 81 + 39 \\ 81 &= 2 \times 39 + 3 \\ 39 &= 13 \times 3 + 0. \end{aligned}$$

The HCF of 201 and 81 is therefore 3. It follows that 201 and 81 are not coprime, and hence that 81 does not have a multiplicative inverse in $\mathbb{Z}_{201}$.

Solution to Exercise A97

(a) Euclid's Algorithm gives

$$\begin{aligned}16 &= 2 \times 7 + 2\\ 7 &= 3 \times 2 + 1.\end{aligned}$$

Starting with the last equation, we have

$$\begin{aligned}1 &= 7 - 3 \times 2\\ &= 7 - 3(16 - 2 \times 7)\\ &= -3 \times 16 + 7 \times 7.\end{aligned}$$

Hence $7 \times 7 = 3 \times 16 + 1$, so $7 \times_{16} 7 = 1$ and therefore $7^{-1} = 7$ in $\mathbb{Z}_{16}$.

(b) Euclid's Algorithm gives

$$\begin{aligned}51 &= 6 \times 8 + 3\\ 8 &= 2 \times 3 + 2\\ 3 &= 1 \times 2 + 1.\end{aligned}$$

Starting with the last equation, we have

$$\begin{aligned}1 &= 3 - 2\\ &= 3 - (8 - 2 \times 3)\\ &= -8 + 3 \times 3\\ &= -8 + 3(51 - 6 \times 8)\\ &= 3 \times 51 - 19 \times 8.\end{aligned}$$

Hence $(-19) \times 8 \equiv 1 \pmod{51}$, but $-19 + 51 = 32$ so

$$32 \times 8 \equiv 1 \pmod{51}.$$

Hence $32 \times_{51} 8 = 1$, so $8^{-1} = 32$ in $\mathbb{Z}_{51}$.

Solution to Exercise A98

(a) The given equation is

$$7 \times_{16} x = 3.$$

Multiplying both sides by the multiplicative inverse of 7 in $\mathbb{Z}_{16}$, which is 7, gives

$$7 \times_{16} 7 \times_{16} x = 7 \times_{16} 3$$

that is,

$$1 \times_{16} x = x = 7 \times_{16} 3.$$

Since $7 \times 3 = 21 = 16 + 5$, we have $x = 5$.

Thus the equation $7 \times_{16} x = 3$ has solution $x = 5$.

(b) The given equation is

$$8 \times_{51} x = 19.$$

Multiplying both sides by the multiplicative inverse of 8 in $\mathbb{Z}_{51}$, which is 32, gives

$$32 \times_{51} 8 \times_{51} x = 32 \times_{51} 19,$$

that is,

$$1 \times_{51} x = x = 32 \times_{51} 19.$$

Since $32 \times 19 = 608 = 510 + 98 = 510 + 51 + 47$, we have $x = 47$.

Thus the equation $8 \times_{51} x = 19$ has solution $x = 47$.

Solution to Exercise A99

(a) Observe that $2 \equiv 15 \pmod{13}$, and we know $5 \times 3 = 15$ so we have

$$5 \times 3 \equiv 2 \pmod{13}.$$

Hence the solution of the given equation is $x = 3$.

Alternatively, $5^{-1} = 8$ in $\mathbb{Z}_{13}$ (since $5 \times 8 = 40 = 39 + 1$, so $5 \times_{13} 8 = 1$). We have $8 \times 2 = 16 = 13 + 3$, so $x = 8 \times_{13} 2 = 3$.

(b) Observe that $5 \equiv -6 \pmod{11}$, and we know $3 \times (-2) = -6$ so we have

$$3 \times (-2) \equiv 5 \pmod{11}.$$

The integer -2 is not an element of $\mathbb{Z}_{11}$, but $-2 \equiv 9 \pmod{11}$.

Hence the solution of the given equation is $x = 9$.

Alternatively, $3^{-1} = 4$ in $\mathbb{Z}_{11}$ (since $3 \times 4 = 12 = 11 + 1$, so $3 \times_{11} 4 = 1$). We have $4 \times 5 = 20 = 11 + 9$, so $x = 4 \times_{11} 5 = 9$.

Solution to Exercise A100

(a) The HCF of 9 and 12 is $d = 3$, and this is also a factor of 6, so the equation $9 \times_{12} x = 6$ has $d = 3$ solutions.

To find the smallest solution of the given equation, we solve the equation

$$\frac{9}{3} \times_{\frac{12}{3}} x = \frac{6}{3},$$

that is,

$$3 \times_4 x = 2.$$

By trying possibilities, we find that this equation has solution $x = 2$, since $3 \times 2 = 6$ and $6 \equiv 2 \pmod 4$. Also $n/d = 12/3 = 4$, so the other solutions are $x = 2 + 4 = 6$ and $x = 2 + 2 \times 4 = 10$.

(b) The HCF of 8 and 12 is 4, but this is not a factor of 7, so the equation $8 \times_{12} x = 7$ has no solutions.

(c) The HCF of 5 and 12 is 1; that is, they are coprime. Hence the equation $5 \times_{12} x = 2$ has a unique solution.

The solution, $x = 10$, can be found in various ways: for example

- by noticing that $5 \times 5 = 25$ and $25 \equiv 1 \pmod{12}$, so $5^{-1} = 5$ in $\mathbb{Z}_{12}$ and therefore $x = 5^{-1} \times_{12} 2 = 10$
- by spotting that $2 \equiv -10 \pmod{12}$, so $5 \times (-2) \equiv 2 \pmod{12}$, and since $-2 \equiv 10 \pmod{12}$ we have $5 \times_{12} 10 = 2$
- by testing possible values for x.

(d) The HCF of 4 and 16 is $d = 4$, and this is also a factor of 12, so the equation $4 \times_{16} x = 12$ has $d = 4$ solutions.

To find the smallest solution of the given equation, we solve the equation

$$\frac{4}{4} \times_{\frac{16}{4}} x = \frac{12}{4},$$

that is,

$$1 \times_4 x = 3,$$

which simplifies to the solution $x = 3$.

Also $n/d = 12/3 = 4$, so the other solutions are $x = 3 + 4 = 7$, $x = 3 + 2 \times 4 = 11$ and $x = 3 + 3 \times 4 = 15$.

(e) The HCF of 3 and 16 is 1; that is, they are coprime. Hence the equation $3 \times_{16} x = 13$ has a unique solution.

The solution, $x = 15$, can be found in various ways. For example, you could test possible values for x: you would eventually find that

$$3 \times 15 = 45 = 2 \times 16 + 13$$

so $3 \times_{16} 15 = 13$. Alternatively, you might spot that $13 \equiv -3 \pmod{16}$, so

$$3 \times (-1) \equiv 13 \pmod{16}$$

which gives

$$3 \times 15 \equiv 13 \pmod{16},$$

and hence $3 \times_{16} 15 = 13$. Alternatively again, you might start by finding the multiplicative inverse of 3 in $\mathbb{Z}_{16}$; a quick way to do this is to observe that $3 \times 11 = 33 \equiv 1 \pmod{16}$, so $3^{-1} = 11$ in $\mathbb{Z}_{16}$. This gives $x = 3^{-1} \times_{16} 13 = 15$.

(f) The HCF of 8 and 16 is 8, but this is not a factor of 2, so the equation $8 \times_{16} x = 2$ has no solutions.

Unit A3

Mathematical language and proof

Introduction

This unit gives an introduction to mathematical proof. While you have already met proofs in your previous mathematical studies, the emphasis of your studies is likely to have been not on proofs, but on problems that can be solved by, essentially, *computing* a result.

In this module the emphasis shifts to a more abstract approach to mathematics, where the goal is to describe clearly properties of mathematical objects using mathematical statements, and to establish their correctness using proofs.

Section 1 introduces the language used to express mathematical statements and reviews the ways in which statements can be combined. Sections 2 and 3 introduce various techniques for proving that a mathematical statement is true. As a further introduction to abstract mathematical thinking, Section 4 introduces the concept of an *equivalence relation* on a set. Equivalence relations are important in many areas of mathematics. You will meet them again in the group theory units of this module.

1 Mathematical statements

In Units A1 *Sets, functions and vectors* and A2 *Number systems* you have seen many examples of mathematical statements, theorems and proofs. In this section you will look in detail at mathematical statements and the ways in which they can be combined and negated. This sets the scene for Sections 2 and 3, where you will learn about methods of proof.

1.1 Statements and negations

The building blocks of mathematical theorems and proofs are assertions called **statements**, also known as **propositions**. In mathematics, a statement is an assertion that is either true or false, though we may not know which. The following are examples of statements.

1. The equation $2x - 3 = 0$ has solution $x = \frac{3}{2}$.
2. $1 + 1 = 3$.
3. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for each positive integer n.
4. There is a real number x such that $\cos x = x$.
5. Every even integer greater than 2 is the sum of two prime numbers.
6. x is greater than 0.

In this list, Statement 1 is true and Statement 2 is false. Statements 3 and 4 are both true, though this is probably not immediately obvious to you in either case. We shall prove that Statement 3 is true later in this section. You can check that Statement 4 is true by noting that the graphs of $y = \cos x$ and $y = x$ intersect; a rigorous proof can be obtained by using the *Intermediate Value Theorem*, which you will meet in the analysis units of this module. At the time of writing it is not known whether Statement 5 is true or false; it is known as *Goldbach's Conjecture*, and mathematicians have been trying to prove it since 1742.

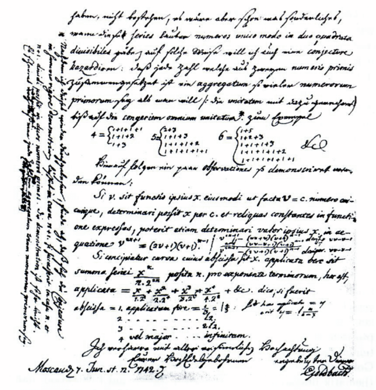


Figure 1 Extract from Goldbach's letter to Euler

On 7 June 1742 the German mathematician Christian Goldbach (1690–1764) posed his conjecture in a letter to Leonhard Euler (1707–1783). An extract from this letter is shown in Figure 1. In the same letter Goldbach also proposed what is now known as the *Weak Goldbach Conjecture*. This states that every odd number greater than 5 can be expressed as the sum of three primes. The Weak Goldbach Conjecture was proved by the Peruvian mathematician Harald Helfgott in 2013. Goldbach and Euler first met at the St Petersburg Academy of Sciences in 1727 when Euler was appointed to a position in the mathematics division, and where Goldbach was professor of mathematics. After Goldbach moved to Moscow in 1729 they began a correspondence which lasted 35 years.

Statement 6 is a little different from the others, since whether it is true or false depends on the value of the variable x. A statement, such as this one, that is either true or false depending on the value of one or more variables, is called a **variable proposition**. We usually denote statements by the capital letters P, Q, R, $\dots$, and we denote variable propositions containing the variable x by $P(x)$, $Q(x)$, $\dots$.

When considering a variable proposition, we must have in mind a suitable set of values from which the possible values of the variable are taken. For example, the set associated with Statement 6 might be $\mathbb{R}$, since for each real number x the assertion is either true or false. A variable proposition with several variables may have several such associated sets. Often the set or sets associated with a variable are clear from the context and so we do not state them explicitly. In particular, unless it is stated otherwise, we assume that if the variable is x or y, then the associated set is $\mathbb{R}$, whereas if the variable is n or m, then the associated set is $\mathbb{Z}$ or $\mathbb{N}$, depending on the context.

An example of an assertion that is not a mathematical statement is '$\{1, 2\}$ is greater than 0'. Since $\{1, 2\}$ is a set, and sets cannot be greater than (nor less than or equal to) zero, the assertion is meaningless, and therefore is neither true nor false. Other examples are 'π is interesting' and '1000 is a large number', which are not precise enough to be either true or false.

Exercise A101

Determine whether each of the following assertions is a mathematical statement. For those that are mathematical statements, state whether or not they are variable propositions.

(a) n is even or n is prime.

(b) The set of odd integers less than 3 is small.

(c) $\{1, 2, 3, 4\}$ is odd.

(d) $\{1, 2, 3, 4\} \cap \{6, 7, 8, 9\} \neq \varnothing$.
(Remember that $\varnothing$ denotes the empty set.)

A **theorem** is simply a mathematical statement that is true. However, we usually reserve the word for a statement that is considered to be of some importance, and whose truth is not immediately obvious, but instead has to be proved. A **proposition** is a 'less important' theorem, and a **lemma** is a theorem that is used in the proof of other theorems. A **corollary** is a theorem that follows from another theorem by a short additional argument. Theorems are sometimes called *results*.

As you may have noticed, we have used the word *proposition* in two quite different ways in this subsection. It can either mean a 'less important' theorem, as just explained, or it can be used with the same meaning as the word 'statement' (this is its meaning in the phrase 'variable proposition'). Both meanings are in common use in mathematics, so you should be aware of them both. Normally, the intended meaning will be clear from the context.

Every statement has a related statement, called its **negation**, which is true when the original statement is false, and false when the original statement is true. The negation of a statement P can usually be written as 'it is not the case that P', but there are often better, more concise ways to express a negation. Thus, for example, the negation of the variable proposition

x is greater than 0

can be written as

it is not the case that x is greater than 0,

but is better expressed as

x is not greater than 0

or even as

$$x \leq 0.$$

We usually denote the negation of a statement P by 'not P'. The process of finding the negation of a statement is called **negating** the statement. Here are some more examples.

Worked Exercise A45

Express concisely the negations of each of the following statements.

(a) There are at least 10 two-digit natural numbers less than 20.

(b) π is less than 5.

Solution

(a) The negation can be expressed as

There are at most 9 two-digit natural numbers less than 20,

or as

There are fewer than 10 two-digit natural numbers less than 20.

(b) The negation can be expressed as

π is greater than or equal to 5,

or as

$$\pi \geq 5.$$

Exercise A102

Express concisely the negations of each of the following statements.

(a) $x = \frac{3}{5}$ is a solution of the equation $3x + 5 = 0$.

(b) The equation $n^2 + n - 2 = 0$ has exactly two solutions.

In the rest of this section you will learn about the possible structures of mathematical statements and their negations.

1.2 Conjunctions and disjunctions

Statements can be combined in various ways to give more complicated statements.

Inserting the word 'and' between two statements P and Q gives a new statement, called the **conjunction** of P and Q, which is true if both of P and Q are true, and false if at least one of P or Q is false.

For example, the variable proposition

x is greater than 0 and x is an integer

is true if *both* of the statements 'x is greater than 0' and 'x is an integer' are true, and false otherwise. Thus the combined statement is true if $x = 4$ but false if $x = 3.5$.

It is sometimes necessary to rephrase a statement to recognise that it is a conjunction. For example, a statement of the form 'P but not Q' is in fact the conjunction 'P and not Q'. Thus, the statement

2 is prime but it is not odd

can be treated as the conjunction '2 is prime and 2 is not odd'.

Inserting the word 'or' between two statements P and Q also gives a new statement, the **disjunction** of P and Q, which is true if at least one of P or Q is true, and false if both of P and Q are false. Thus, the word 'or' is used in its inclusive sense in mathematical statements: 'P or Q' means 'either P or Q or possibly both'.

For example, the variable proposition

x is greater than 0 or x is an integer

is true if *at least one* of the statements 'x is greater than 0' and 'x is an integer' is true, and false otherwise. Thus this combined statement is true if $x = 4$, $x = 3.5$ or $x = -4$ but false if $x = -3.5$.

Just as for conjunctions, it may be necessary to rephrase a statement to recognise that it is a disjunction. For example, statements of the form 'at least one of P or Q holds', or 'either P, or Q', are different ways of expressing the disjunction 'P or Q'. So the statement

at least one of m or n is odd

can be treated as the disjunction

m is odd or n is odd.

Negating conjunctions and disjunctions

Since the statement 'P and Q' is true exactly when both P and Q are true, its negation is true when at least one of P or Q is false. Thus the negation of 'P and Q' is the statement 'not P or not Q'.

Worked Exercise A46

Negate the following conjunctions.

(a) n is positive and p is prime

(b) The sets A and B are both empty.

(c) p is an odd prime.

Solution

(a) This statement is false when at least one of 'n is positive' and 'p is prime' is false.

The negation is

n is less than or equal to 0, or p is not prime.

(b) This statement can be expressed as

The set A is empty and the set B is empty.

The statement is false when at least one of 'the set A is empty' and 'the set B is empty' is false.

The negation is

The set A is non-empty or the set B is non-empty.

(c) This statement can be expressed as

p is odd and p is a prime.

The statement is false when at least one of 'p is odd' and 'p is a prime' is false.

The negation is

p is even or p is not prime.

Similarly, the negation of 'P or Q' is true exactly when both of P and Q are false; that is, exactly when 'not P and not Q' is true. A little thought and some examples should convince you of this.

Worked Exercise A47

Negate the following disjunctions.

(a) Either m or $m+1$ is even

(b) $x \geq 0$ or $y \geq 0$

(c) Either $A = B$ or $A \cap B = \varnothing$.

Solution

(a) This statement can be expressed as

m is even or $m + 1$ is even.

The statement is false when both 'm is even' and '$m + 1$ is even' are false.

The negation is

m is odd and $m + 1$ is odd.

(b) This statement is false when both '$x \geq 0$' and '$y \geq 0$' are false.

The negation is

$x < 0$ and $y < 0$.

(c) This statement is false when both '$A = B$' and '$A \cap B = \varnothing$' are false.

The negation is

$A \neq B$ and $A \cap B \neq \varnothing$.

Exercise A103

Express concisely the negations of each of the following statements.

(a) Both x and y are integers.

(b) The integer m is even but the integer n is odd.

(c) At least one of the integers m or n is odd.

(d) Either $A = \varnothing$ or $B = \varnothing$.

1.3 Implications

Many mathematical statements are of the form 'if something, then something else', for example:

if $x > 2$, then $x^2 > 4$.

This type of statement is called an **implication**. An implication is made up of two statements, which in the example above are '$x > 2$' and '$x^2 > 4$', and can be expressed by combining these statements using the words 'if' and 'then'. In an implication 'if P, then Q', the statement P is called the **hypothesis** of the implication, and the statement Q is called the **conclusion**.

It is important to be clear about exactly what an implication asserts. The statement above asserts only that if you know that $x > 2$, then you can be sure that $x^2 > 4$. It does not assert anything about the truth or falsity of '$x^2 > 4$' when x is not greater than 2. In general, the implication

if P, then Q

asserts that if P is true, then Q is also true; that is, that it cannot happen that P is true and Q is false. The implication does not assert anything about the truth or falsity of Q when P is false.

If x is a real variable, then the statement

if $x > 2$, then $x^2 > 4$

is true because for every real number x for which '$x > 2$' is true, '$x^2 > 4$' is also true. Strictly speaking, this statement should be expressed as

for all $x \in \mathbb{R}$, if $x > 2$, then $x^2 > 4$.

However, it is conventional to omit the initial 'for all $x \in \mathbb{R}$', and interpret the statement as if it were there. We adopt this convention throughout this module (indeed, it is used in almost all mathematical texts), so statements of the form 'if P, then Q', where P and/or Q are variable propositions, should be interpreted as applying to all possible values of the variables in the statements P and Q.

An implication does not have to be expressed using the words 'if' and 'then' – there are many other ways to convey the same meaning. The left-hand side of the table below lists some ways of expressing the implication 'if P, then Q'. The right-hand side gives examples for the particular implication 'if $x > 2$, then $x^2 > 4$'.

Ways of writing 'if P, then Q'	Ways of writing 'if $x > 2$, then $x^2 > 4$'
P implies Q	$x > 2$ implies $x^2 > 4$
$P \implies Q$	$x > 2 \implies x^2 > 4$
P is sufficient for Q	$x > 2$ is sufficient for $x^2 > 4$
P only if Q	$x > 2$ only if $x^2 > 4$
Q whenever P	$x^2 > 4$ whenever $x > 2$ (or: $x^2 > 4$, for all $x > 2$)
Q follows from P	$x^2 > 4$ follows from $x > 2$
Q is necessary for P	$x^2 > 4$ is necessary for $x > 2$
Q provided that P	$x^2 > 4$ provided that $x > 2$

The symbol $\implies$ is read as 'implies', and it is commonly used in mathematical notation. The form 'P only if Q' may seem strange at first; it asserts that the only circumstance in which P can be true is if Q is also true. In other words, if P is true, then Q must also be true – that is, P implies Q.

The notation $\implies$ was first used by Nicolas Bourbaki in 1954. Nicolas Bourbaki was the pseudonym for a group of (mainly French) mathematicians who from 1935 over a period of thirty years produced an influential series of textbooks that were designed to present all of pure mathematics in a completely structured and axiomatic way. The name Bourbaki derives from that of a nineteenth-century French general, Charles Bourbaki, and was adopted by the group as a reference to a prank lecture by a student.

The founders of the Bourbaki group

The next exercise is for you to practise working with implications. In Section 2 you will see how to formally prove or disprove statements like those in parts (b) and (c). Whether the statement in part (a) is true or false can be established by algebraic manipulation.

Exercise A104

Rewrite each of the following statements in the form 'if P, then Q'. In each case, state whether you think the implication is true. You are not asked to justify your answers.

(a) $x^2 - 2x + 1 = 0 \implies (x-1)^2 = 0$.

(b) Whenever n is odd, so is n^3.

(c) Every integer that is divisible by 3 is also divisible by 6.

(d) $x > 2$ only if $x > 4$.

(e) $x^3 \leq 0$ provided that $x \leq 0$.

Many theorems have statements of the form 'Let P. Then Q'. This is an alternative way to express a theorem of the form 'if P, then Q'. You have already met several theorems stated in this form – for example, the Division Theorem (Theorem A9 in Unit A2).

Theorem A9 Division Theorem

Let a and n be integers, with $n > 0$. Then there are unique integers q and r such that

$$a = qn + r, \quad \text{with } 0 \leq r < n.$$

The theorem could be restated as follows.

Theorem A9 Division Theorem (version 2)

If a and n are integers, with $n > 0$, then there are unique integers q and r such that

$$a = qn + r, \quad \text{with } 0 \leq r < n.$$

The negation of an implication

Contrary to what you might expect, the negation of an implication is *not* another implication – rather, it is a conjunction. To see why, it might help to think about the implication

if P, then Q

as asserting

it is not the case that P is true and Q is false.

Thus, *negating* the implication is equivalent to asserting that it *is* the case that P is true and Q is false, which is the conjunction

P and not Q.

A non-mathematical example might be helpful here. Consider the statement

If it snows before the next train to London is due to leave, then the next train to London gets cancelled.

If you want to negate this statement, you need to think about what has to happen in order for it to be false: that occurs if it snows before the next train to London is due to leave and the train leaves anyway. So the negation is

It snows before the next train to London is due to leave, and the next train to London does not get cancelled.

You will need to work with negations of implications when you meet *counterexamples* later in Section 2, so it will help to practise negating implications with mathematical content. This is the topic of the next worked exercise and exercise.

Here and later in the unit, we sometimes use brackets to avoid ambiguity when the conclusion of an implication is a conjunction or a disjunction. For example, in the implication

if the product mn is odd, then (m is odd and n is odd),

the conclusion is the conjunction 'm is odd and n is odd'. Enclosing this conclusion in brackets eliminates any possible confusion with the conjunction of the implication

if the product mn is odd, then m is odd

and the statement 'n is odd'.

Worked Exercise A48

Write down the negations of each of the following implications.

(a) If m is odd, then m^2 is even.

(b) If m divides 12, then (m divides 3 or m divides 4).

Solution

(a) The statement 'if m is odd, then m^2 is even' can be restated as 'it is not the case that m is odd and m^2 is not even'.

The negation is

m is odd and m^2 is not even,

that is,

m is odd and m^2 is odd.

(b) The implication has the form 'if m divides 12, then Q', where Q is the statement 'm divides 3 or m divides 4'. We can restate the implication in the form 'it is not the case that (m divides 12 and not Q)'.

The negation of 'm divides 3 or m divides 4' is

m does not divide 3 and m does not divide 4.

Therefore the negation of the implication is

m divides 12, and m divides neither 3 nor 4.

Exercise A105

Write down the negations of each of the following implications.

(a) If m and n are odd, then $m + n$ is odd.

(b) If $A = \varnothing$, then ($A \cup B = \varnothing$ or $B - A = \varnothing$).

(For part (b), remember that $B - A$ denotes the set of elements of B that are not elements of A.)

The converse of an implication

Given any implication, we can form another implication, called its **converse**. The converse of the implication 'if P, then Q' is the implication

if Q, then P.

For example, the converse of the implication

if $x > 2$, then $x^2 > 4$

is

if $x^2 > 4$, then $x > 2$.

In this example, the original implication is true, and its converse is false (to see that the converse is false consider, for example, $x = -3$). It is also possible for an implication and its converse to be both true, or both false. In other words, knowledge of whether an implication is true or false tells you *nothing at all* about whether its converse is true or false. You should remember this important fact whenever you read or write implications.

To help you remember these facts about implications, you may again find it helpful to consider non-mathematical examples. For example, the implication

if Rosie is a sheep, then Rosie is less than two metres tall

is true, but its converse,

if Rosie is less than two metres tall, then Rosie is a sheep,

certainly is not true!

Exercise A106

For each of the following implications about integers m and n, write down its converse and state whether you think the implication, its converse or both are true. You are not asked to justify your answers.

(a) If m and n are both odd, then $m + n$ is even.

(b) If one of the pair m, n is even and the other is odd, then $m + n$ is odd.

The contrapositive of an implication

Given any implication, we can form a further implication, called its **contrapositive**. Unlike the converse, the contrapositive is *equivalent* to the original implication. The contrapositive of the implication 'if P, then Q' is

if not Q, then not P.

For example, the contrapositive of the implication

if x is an integer, then x^2 is an integer

is the implication

if x^2 is not an integer, then x is not an integer.

You can think of an implication and its contrapositive as asserting the same thing, but in different ways. You should take a few moments to convince yourself of this in the case of the example just given.

Try this also with the following non-mathematical example. The contrapositive of the implication

if Rosie is a sheep, then Rosie is less than two metres tall

is

if Rosie is not less than two metres tall, then Rosie is not a sheep,

or, more simply,

if Rosie is at least two metres tall, then Rosie is not a sheep.

Contrapositive implications are a key ingredient of an important method of proof, proof by *contraposition*, that you will meet in Subsection 3.2. For now, it is important to remember the distinction between the converse of an implication, which is *not* equivalent to the implication, and its contrapositive, which is. A little practice should help you remember this distinction.

Exercise A107

For each of the following implications about integers m and n, write down its converse and its contrapositive and state whether you think the converse, the contrapositive or both are true. You are not asked to justify your answers.

(a) If the product mn is even, then at least one of m or n is even.

(b) If q divides the product mn, then (q divides m or q divides n).

1.4 Equivalences

The statement

if P, then Q, and if Q, then P,

which asserts that the implication 'if P, then Q' and its converse are *both* true, is usually expressed more concisely as

P if and only if Q.

Recall that 'P if Q' means '$Q \implies P$', and 'P only if Q' means '$P \implies Q$', so the phrase 'if and only if' is rather natural in this context.

If the statement 'P if and only if Q' is true, then P and Q are either both true or both false – in other words, if either one of P or Q is true, then so is the other.

Here are two examples:

1. n is odd if and only if n^2 is odd
2. $x > 2$ if and only if $x^2 > 4$.

Statements like these are called **equivalences**.

Equivalence 1 above is true because both the implications 'if n is odd, then n^2 is odd' and 'if n^2 is odd, then n is odd' are true. However, equivalence 2 is false because the implication 'if $x^2 > 4$, then $x > 2$' is false.

You have met equivalences before. For example, the Factor Theorem (Theorem A2 in Unit A2) contains an equivalence in its statement.

Theorem A2 Factor Theorem (in $\mathbb{R}$)

Let $p(x)$ be a real polynomial, and let $\alpha \in \mathbb{R}$. Then $p(\alpha) = 0$ if and only if $x - \alpha$ is a factor of $p(x)$.

As with implications, there are many different ways to express equivalences. The table below lists some ways in which this can be done, with illustrations using example 1 above.

Ways of writing 'P if and only if Q'	Ways of writing 'n is odd if and only if n^2 is odd'
$P \iff Q$	n is odd $\iff$ n^2 is odd
P is equivalent to Q	n is odd is equivalent to n^2 is odd
P is necessary and sufficient for Q	n is odd is necessary and sufficient for n^2 to be odd

The symbol $\iff$ is commonly used to denote equivalences. It is usually read as 'if and only if', or sometimes as 'is equivalent to'.

It is important to remember that the symbol $\iff$ denotes equivalence between statements rather than equality between expressions, and should never be used in place of $=$. For example, it is *incorrect* to write $x^2 - 1 \iff (x+1)(x-1)$, but correct to write either

$$x^2 - 1 = (x+1)(x-1),$$

or

$$x^2 - 1 = 0 \iff (x+1)(x-1) = 0.$$

Exercise A108

For each of the following equivalences about integers, write down the two implications that it asserts, state whether you think each implication is true and hence state whether you think the equivalence is true. You are not asked to justify your answers.

(a) The product mn is odd if and only if both m and n are odd.

(b) The product mn is even if and only if both m and n are even.

In some cases, it is helpful to think of the equivalence $P \iff Q$ in terms of $P \implies Q$ and the implication 'not $P \implies$ not Q'. Recall that $Q \implies P$ is equivalent to its contrapositive 'not $P \implies$ not Q'. Therefore, since $P \iff Q$ asserts that both $P \implies Q$ and $Q \implies P$ hold, an alternative way to express the equivalence is to assert both

$$P \implies Q \text{ and } (\text{not } P \implies \text{not } Q).$$

For example, the equivalence

$$m \text{ is even} \iff m^2 \text{ is even}$$

can be expressed as

$$(m \text{ is even} \implies m^2 \text{ is even}) \text{ and } (m \text{ is odd} \implies m^2 \text{ is odd}).$$

Theorem A11 in Unit A2 contains an equivalence stated in this form.

Theorem A11

Let n and a be positive integers, with a in $\mathbb{Z}_n$.

- If a and n are coprime, then a has a multiplicative inverse in $\mathbb{Z}_n$.
- If a and n are not coprime, then a does not have a multiplicative inverse in $\mathbb{Z}_n$.

Thus, this theorem can be stated more succinctly as follows.

Theorem A11 (version 2)

Let n and a be positive integers, with a in $\mathbb{Z}_n$. Then a has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a and n are coprime.

We will prove this theorem in Subsection 3.1.

Although a mathematical statement should normally be interpreted as meaning precisely what it says – no more and no less – there is one common exception to this rule. When giving a *definition*, we usually write 'if' when we really mean 'if and only if'. You have seen many examples of definitions in this form throughout Units A1 and A2 – below are two specific ones.

Definition

A set A is a subset of a set B if each element of A is also an element of B.

This definition (from Subsection 2.5 of Unit A1) is really stating that the two statements

A is a subset of B

and

each element of A is also an element of B

are *equivalent*. Below is the second example (from Subsection 3.2 of Unit A2).

Definition

Let n be a positive integer. Two integers a and b are **congruent modulo n** if $a - b$ is a multiple of n; that is, if a and b have the same remainder on division by n.

Again, this definition is really saying that the statements 'a and b are congruent modulo n' and '$a - b$ is a multiple of n' are equivalent.

1.5 Universal and existential statements

Many mathematical statements include the phrase 'for all', or another expression with the same meaning. Here are a few examples.

1. $x^2 \geq 0$ *for all* real numbers x.
2. *Every* multiple of 6 is divisible by 3.
3. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ *for each* positive integer n.
4. *Any* rational number is a real number.

Statements of this type are known as **universal** statements, and the phrase 'for all', and its equivalents, are referred to as the **universal quantifier**.

The universal quantifier is sometimes denoted by the symbol $\forall$; for example, the first universal statement above might be abbreviated as

$$\forall x \in \mathbb{R},\ x^2 \geq 0,$$

which is read as 'for all x in $\mathbb{R}$, x squared is greater than or equal to zero'.

Statements that begin with a phrase like 'There are no ...' or 'There does not exist ...' are universal statements because they can be rephrased in terms of 'for all'. For example, the statement

there is no integer n such that $n^2 = 3$

can be rephrased as

for all integers n, $n^2 \neq 3$.

In Subsection 1.3 you met an important class of universal statements. Recall that implications of the form

$$P(x) \implies Q(x),$$

should strictly be expressed as 'for all x, if $P(x)$, then $Q(x)$', but the initial 'for all x' is generally omitted by convention. So implications where the hypothesis and the conclusion are variable propositions are in fact universal statements where the universal quantifier is omitted. For example, the statement

if n is a multiple of 6, then n is a multiple of 3

means in fact

for all integers n, if n is a multiple of 6, then n is a multiple of 3.

We now turn to another type of statement with a quantifier. Some mathematical statements include the phrase 'there exists', or another expression with the same meaning. Here are a few examples.

1. *There exists* a real number that is not a rational number.
2. *There is* a real number x such that $\cos x = x$.
3. *Some* multiples of 3 are not divisible by 6.
4. The equation $x^3 + x^2 + 5 = 0$ has *at least one* real solution.

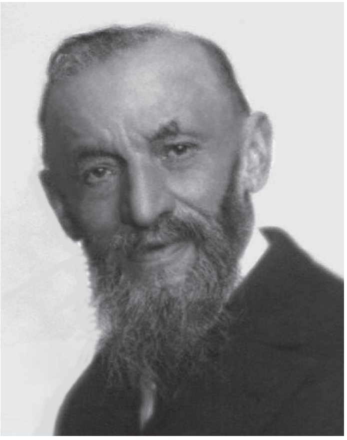
Statements of this type are known as **existential** statements, and the phrase 'there exists' and its equivalents are referred to as the **existential quantifier**.

In the third example, the word *some* is used to mean 'at least one', rather than several. It is important to remember that this is the standard mathematical usage of 'some'.

The existential quantifier is sometimes denoted by the symbol $\exists$; for example, the second existential statement above might be abbreviated as

$\exists x \in \mathbb{R}$ such that $\cos x = x$,

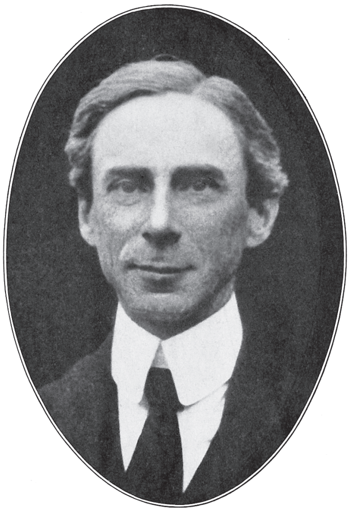
which is read as 'there exists x in $\mathbb{R}$ such that $\cos x$ equals x'.



Giuseppe Peano

The symbol $\exists$ was introduced by Giuseppe Peano (1858–1932) in 1897 and was used by Bertrand Russell (1872–1970) and Alfred North Whitehead (1861–1947) in their monumental *Principia Mathematica* (1910–1913). In 1935 Gerhard Gentzen (1909–1945) introduced the $\forall$ symbol. He called it the All-Zeichen (all character), in analogy with $\exists$ which Gentzen said he borrowed from Russell.

In natural language, the word 'any' can mean either 'every' or 'at least one', as in 'any fool could do that' and 'did you win any prizes?'. In mathematics, the meaning depends on the context in a similar way. We try to avoid using 'any' where it might cause confusion.



Bertrand Russell

As already mentioned, it is often necessary to negate statements; for example, this is the case when we consider proof by contradiction or proof by contraposition, which you will meet in Section 3. The negation of universal and existential statements needs to be treated with particular care. The negation of a universal statement is an existential statement, and vice versa. This is illustrated by the examples in the table below.

Statement	Negation
Every integer is a real number.	There exists an integer that is not a real number.
There is an even prime number.	Every prime number is odd.
The equation $x^2 + 4 = 0$ has a real solution.	For all real numbers x, $x^2 + 4 \neq 0$.

Exercise A109

Express concisely the negations of each of these statements.

(a) There is a real number x such that $\cos x = x$.

(b) There exists an integer that is divisible by 3 but not by 6.

(c) Every real number x satisfies the inequality $x^2 \geq 0$.

Gerhard Gentzen

You have now met the negations of a number of different types of statements, and to conclude this section we collect them together in the table below.

Statement	Negation
P	not P
P and Q	not P or not Q
P or Q	not P and not Q
If P, then Q	P and not Q
For all x, P	There exists an x such that not P
There exists an x such that P	For all x, not P

2 Direct proof

The aim of this section and the next is to make you more familiar with the structures of various different types of mathematical proof. This section deals with *direct* methods of proof – that is, methods of proof which involve a series of logical steps leading from known facts and assumptions directly to the statement you wish to prove. In the next section you will consider *indirect* methods of proof.

Working through proofs, producing your own proofs and critically assessing mathematical arguments should help you to express your own mathematical thoughts and ideas more clearly.

In this module the proofs that you are asked to produce are simpler than many of the ones that are provided for you to read. Do not be discouraged if proof writing seems difficult at first: it is a skill that is acquired gradually. Working through the proofs that you meet is probably the most useful preparation. It is also important to study the more complex proofs that appear later in the module, and understand why they prove the statements that they claim to prove.

A *proof* of a mathematical statement is a logical argument that establishes that the statement is true. Here is a simple example.

Worked Exercise A49

Prove the following statement.

If n is an odd number between 0 and 10, then n^2 is also odd.

Solution

The odd numbers between 0 and 10 are 1, 3, 5, 7 and 9. The squares of these numbers are 1, 9, 25, 49 and 81, respectively, and these are all odd.

In the example above, there were only a small number of possibilities to consider, so it was easy to prove the statement by considering each one in turn. This method of proof is known as **proof by exhaustion** because we exhaust all possibilities. In contrast, it is not possible to prove the statement 'If n is an odd number, then n^2 is also odd' using proof by exhaustion because there are infinitely many possibilities to consider. Most mathematical statements that you will come across cannot be proved by exhaustion because there are too many possibilities to consider – usually infinitely many. Instead we must supply a general proof.

As an initial example of a general proof, we state and prove a result that applies to expressions of the form $a^n - b^n$. These expressions occur often in calculations, and you have probably already met the factorisations

$$a^2 - b^2 = (a-b)(a+b),$$
$$a^3 - b^3 = (a-b)(a^2+ab+b^2),$$
$$a^4 - b^4 = (a-b)(a^3+a^2b+ab^2+b^3),$$

and so on. The following general result can be proved by multiplying out the expression on the right-hand side.

Theorem A12 Geometric Series Identity

Let $a, b \in \mathbb{R}$ and let n be a positive integer. Then

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

Proof Expanding the right-hand side of the equality gives

$$\begin{aligned}
&(a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \\
&\quad = a^n + a^{n-1}b + \cdots + a^2b^{n-2} + ab^{n-1} \\
&\qquad\quad - (a^{n-1}b + a^{n-2}b^2 + \cdots + ab^{n-1} + b^n) \\
&\quad = a^n - b^n,
\end{aligned}$$

as required. ■

The structure of the argument required in most proofs goes beyond the kind of algebraic verification used here. In the rest of this section, you will see how different techniques can be used for proofs that require arguments with a more complex structure.

2.1 Proving implications

Suppose we wish to prove that the implication $P \implies Q$ is true. We have to prove that whenever the statement P is true, the statement Q is also true. Often the best way to do this is to start out by *assuming* that P is true, and proceed as follows. If we know that the statement

$$P \implies P_1$$

is true for some statement P_1, then we can deduce that P_1 is also true. Similarly, if we know that the statement

$$P_1 \implies P_2$$

is true for some statement P_2, then we can deduce that P_2 is also true. In this way we can build up a sequence of statements

$$P, P_1, P_2, \dots,$$

each of which we know to be true under the assumption that P is true. The aim is to build up such a sequence

$$P, P_1, P_2, \dots, P_n, Q,$$

which leads to Q. If this can be achieved, then we have a proof of the implication $P \implies Q$. Here is an example.

Worked Exercise A50

Prove that if n is odd, then n^2 is odd.

Solution

We have to prove that if n is odd, then n^2 is also odd. So we start by assuming that 'n is odd' is true, and make use of the fact that n is odd if and only if it can be written in the form '2 times some integer plus 1'.

Let n be an odd integer. Then

$$n = 2k + 1 \text{ for some integer } k.$$

Hence

$$n^2 = (2k+1)^2 = (2k)^2 + 2(2k) + 1 = 2(2k^2 + 2k) + 1.$$

We see that n^2 is odd because we have shown that n^2 is equal to 2 times some integer (that is, $2k^2 + 2k$) plus 1.

Since $2k^2 + 2k$ is an integer, this shows that n^2 is an odd integer.

In the proof in Worked Exercise A50, statement P is 'n is odd', and we start by assuming that this is true. Assumptions are generally introduced by words such as 'let', 'suppose' or 'assume'. Statement P_1 is '$n = 2k + 1$ for some integer k', and so on. We use words like 'then' and 'hence' to indicate that one statement follows from another. The string of equalities

$$n^2 = \cdots = 2(2k^2 + 2k) + 1$$

in the proof can be regarded either as a sequence of three statements, namely

$$n^2 = (2k + 1)^2,$$
$$n^2 = (2k)^2 + 2(2k) + 1,$$
$$n^2 = 2(2k^2 + 2k) + 1,$$

or as a single statement asserting the equality of all four expressions.

Many of the true statements about odd and even integers that appeared in the exercises in the last subsection can be proved using ideas similar to those of the proof in Worked Exercise A50; that is, we write an odd integer as $2 \times$ some integer $+ 1$, and an even integer as $2 \times$ some integer. (Similarly, we can often prove statements about multiples of 3 by writing each such number as $3 \times$ some integer, and so on.) Here is another example.

Worked Exercise A51

Prove that the sum of two odd integers is even.

Solution

We start by considering two odd integers, and then consider their sum.

Let m and n be odd integers. Then

$$m = 2k + 1 \text{ and } n = 2l + 1 \text{ for some integers } k \text{ and } l.$$

It is important to choose different symbols k and l here. We certainly cannot deduce from the first statement that $m = 2k + 1$ and $n = 2k + 1$ for some integer k; that would be the case only if m and n were equal!

Hence

$$m + n = (2k + 1) + (2l + 1) = 2k + 2l + 2 = 2(k + l + 1).$$

Since $k + l + 1$ is an integer, this shows that $m + n$ is an even integer.

We have seen that a sequence $P, P_1, P_2, \ldots, P_n, Q$ of statements forms a proof of the implication $P \implies Q$ provided that each statement is shown to be true under the assumption that P is true. In Worked Exercises A50 and A51, each statement in the sequence was deduced from the statement

immediately before, but the sequence can also include statements that are deduced from one or more statements further back in the sequence, or statements that we know to be true from our previous mathematical knowledge. This is illustrated by Worked Exercise A52 below.

A fact that you may already know, which will be useful in Worked Exercise A52 and also later in this section, is that every integer greater than 1 has a unique expression as a product of prime numbers. For example, $6468 = 2 \times 2 \times 3 \times 7 \times 7 \times 11$, and this is the only way to express 6468 as a product of primes (except of course that we can change the order of the primes in the expression – the expression is unique *up to* the order of the primes). This fact is known as the *Fundamental Theorem of Arithmetic*.

Theorem A13 Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written as a product of prime numbers. The factorisation is unique up to the order of the factors.

It is certainly not obvious that the Fundamental Theorem of Arithmetic is true! However, a proof is beyond the scope of this module.

Worked Exercise A52

Prove that for every integer n, the number $n^3 + 3n^2 + 2n$ is divisible by 6.

Solution

Let n be an integer. Now

$$n^3 + 3n^2 + 2n = n(n^2 + 3n + 2) = n(n+1)(n+2).$$

Thus $n^3 + 3n^2 + 2n$ is the product of three consecutive integers.

We know that out of any two consecutive integers, one must be divisible by 2, and out of any three consecutive integers, one must be divisible by 3.

It follows that the three factors n, $n+1$ and $n+2$ include at least one that is divisible by 2, and one that is divisible by 3. Thus both the primes 2 and 3 are factors of $n^3 + 3n^2 + 2n$.

Hence (by the Fundamental Theorem of Arithmetic) $n^3 + 3n^2 + 2n$ can be expressed as $2 \times 3 \times r$ for some integer r, and so it is divisible by $6 = 2 \times 3$.

The next exercise gives you practice in the techniques that you have seen so far in this subsection.

Exercise A110

Prove each of the following implications.

(a) If n is an even integer, then n^2 is even.

(b) If m and n are multiples of k, then so is $m+n$.

(c) If one of the pair m, n is odd and the other is even, then $m+n$ is odd.

(d) If n is a positive integer, then n^2+n is even.

If a proof of an implication is particularly simple, and each statement in the sequence follows directly from the one immediately before, then we sometimes present the proof by writing the sequence of statements in the form

$$P \implies P_1 \implies P_2 \implies P_3 \implies \cdots \implies P_n \implies Q.$$

This notation indicates that each of the statements $P \implies P_1$, $P_1 \implies P_2$, $\dots$, $P_n \implies Q$ is true. It is particularly appropriate for proofs that depend mostly on algebraic manipulation. Here is an example.

Worked Exercise A53

Prove that if $x(x-2)=3$, then $x=-1$ or $x=3$.

Solution

$$\begin{aligned} x(x-2)=3 &\implies x^2-2x-3=0 \\ &\implies (x+1)(x-3)=0 \\ &\implies x+1=0 \text{ or } x-3=0 \\ &\implies x=-1 \text{ or } x=3. \end{aligned}$$

It is worth noting that Worked Exercise A53 does not ask us to *solve* the equation, but, rather, to prove the implication

$$x(x-2)=3 \implies x=-1 \text{ or } x=3\,.$$

By proving this implication, we showed that -1 and 3 are the only possibilities for solutions of the equation $x(x-2)=3$. We did not show that -1 and 3 actually *are* solutions, since for that it is necessary to prove also that if $x=-1$ or $x=3$, then $x(x-2)=3$, that is, the *converse* of the given implication. Thus, strictly, we have not *solved* the equation! Whenever we solve an equation, an implication and its converse must both be proved; in other words, we need to prove an equivalence. We will do this for the equation in Worked Exercise A53 in the next subsection (see Worked Exercise A55).

Even though proofs that depend on algebraic manipulation are among the easiest to produce, they still require care, as the following example shows.

Worked Exercise A54

Explain why the following proof that

$$4x^2 = x \implies x = \tfrac{1}{4}$$

is incorrect.

Claim (incorrect!)

If $4x^2 = x$, then $x = \frac{1}{4}$.

Proof (incorrect!)

$$\begin{aligned} 4x^2 = x &\implies 4x = 1 \\ &\implies x = \tfrac{1}{4}. \end{aligned}$$

■

Solution

The problem with this attempt lies in the implication

$$4x^2 = x \implies 4x = 1.$$

This implication is false: if $x = 0$, then the hypothesis $4 \times 0^2 = 0$ is true but the conclusion $4x = 1$ is false.

This happens because we can only divide both sides of the equation by the variable x if we suppose explicitly that $x \neq 0$, and then look separately at the case $x = 0$.

A correct deduction is as follows.

$$\begin{aligned} 4x^2 = x &\implies 4x^2 - x = 0 \\ &\implies x(4x - 1) = 0 \\ &\implies x = 0 \text{ or } x = \tfrac{1}{4}. \end{aligned}$$

Worked Exercise A54 requires a skill that is also helpful in writing proofs, namely the ability to evaluate arguments critically. The next two exercises give you further practice at spotting mistakes in deductions.

In the first of these exercises, and elsewhere later in the unit, you will meet an argument that involves rearranging an inequality. You should be familiar with the rules for rearranging inequalities from your previous mathematical studies, but if you need to refresh your memory, the rules are listed in the module Handbook. Inequalities are especially important in analysis, so you will study them more formally in the first of the analysis units, Unit D1 *Numbers*.

Exercise A111

Explain why the following deduction that $x = -1$ from the assumption $x \leq -1$ is incorrect.

Claim (incorrect!)

If $x \leq -1$, then $x = -1$.

Proof (incorrect!) We have that $x \leq -1 \implies (x+1)^2 \leq 0$, because

$$x \leq -1 \implies x + 1 \leq 0 \implies (x+1)^2 \leq 0\,.$$

However, $(x+1)^2$ is the square of a real number, and a square can never be negative. Hence the only possibility is $x + 1 = 0$, that is, $x = -1$.

Therefore, if $x \leq -1$, then $x = -1$. ■

In the next exercise you are asked to evaluate an incorrect argument that claims to prove a correct statement.

Exercise A112

Consider the following statement.

If $z_1 = 1 + 2i$ and $z_2 = \sqrt{3} - i\sqrt{2}$, then $|z_1| = |z_2|$.

Explain why the argument below is not a correct proof of this statement and write a correct proof.

Proof (incorrect!)

$$\begin{aligned} |z_1| = |z_2| &\implies |z_1|^2 = |z_2|^2 \\ &\implies 1^2 + 2^2 = \left(\sqrt{3}\right)^2 + \left(-\sqrt{2}\right)^2 \\ &\implies 1 + 4 = 3 + 2 \\ &\implies 5 = 5. \end{aligned}$$

Therefore $|z_1| = |z_2|$. ■

The incorrect proof in Exercise A112 shows a common proof pitfall: it is important to remember that assuming the statement P to be proved and using it to deduce a statement that is known to be true provides *no information at all* about the truth of P. Here is an archetypal example of this kind of incorrect argument.

Example (incorrect!)

$$\begin{aligned} 1 = -1 &\implies 1^2 = (-1)^2 \\ &\implies 1 = 1. \end{aligned}$$

In this example the conclusion $1 = 1$ is true, and each step in the deduction is valid, but the original statement, $1 = -1$, is most definitely false! As you learned in Subsection 1.3, an implication $P \implies Q$ does not give any information about the truth or falsity of Q when P is false.

2.2 Proving equivalences

We now discuss how to prove equivalences. Recall that the equivalence 'P if and only if Q' asserts that both the implication '$P \implies Q$' ('P only if Q') and its converse '$Q \implies P$' ('P if Q') are true. The best way to prove 'P if and only if Q' is usually to tackle each implication separately. However, if a simple proof of one of the implications can be found, in which each statement follows from the one before, then it is *sometimes* possible to 'reverse all the arrows' to obtain a proof of the converse implication. That is, if you have found a proof of the form

$$P \implies P_1 \implies P_2 \implies P_3 \implies \cdots \implies P_n \implies Q,$$

then you *may* find that also each of the following implications is true:

$$Q \implies P_n \implies \cdots \implies P_3 \implies P_2 \implies P_1 \implies P.$$

In this case you may be able to present the proofs of both implications at once, by writing

$$P \iff P_1 \iff P_2 \iff P_3 \iff \cdots \iff P_n \iff Q.$$

As with implications, this is particularly appropriate for proofs that depend mostly on algebraic manipulation. The next worked exercise gives a proof of this type showing that the implication in Worked Exercise A53 and its converse are both true. Remember that the symbol $\iff$ is the one to use when solving equations or inequalities.

Worked Exercise A55

Prove that $x(x-2)=3$ if and only if $x=-1$ or $x=3$.

Solution

$$\begin{aligned} x(x-2)=3 &\iff x^2-2x-3=0 \\ &\iff (x+1)(x-3)=0 \\ &\iff x+1=0 \text{ or } x-3=0 \\ &\iff x=-1 \text{ or } x=3. \end{aligned}$$

In Worked Exercise A55 we solved the equation $x(x-2)=3$: we showed that its solution set is $\{-1,3\}$. The forward ($\implies$) part of the proof shows that if x satisfies $x(x-2)=3$, then $x=-1$ or $x=3$; in other words, these are the only possible solutions of the equation. This is what we proved earlier in Worked Exercise A53. The backward ($\impliedby$) part shows that if $x=-1$ or $x=3$, then x satisfies $x(x-2)=3$; in other words, these two values actually are solutions of the equation (note that if you were asked to prove only that $x=-1$ and $x=3$ are solutions, and not that they are the *only* solutions, then it would be more natural to simply substitute each of these values in turn into the equation).

In the next worked exercise you are asked to prove a statement that involves sets. The proof requires a separate argument for each of the two implications that make up the equivalence.

Worked Exercise A56

Let A and B be any sets. Prove that

$$A \cup B = A \iff B \subseteq A.$$

Solution

We prove the $\implies$ direction first; that is, we assume that $A \cup B = A$.

Suppose $A \cup B = A$.

We want to deduce that $B \subseteq A$, that is, that if $x \in B$ then $x \in A$. So we pick an element $x \in B$.

Let $x \in B$. Then x is also in the union $A \cup B$. But since $A \cup B = A$, this implies that $x \in A$. Therefore $B \subseteq A$, so we have shown that $A \cup B = A \implies B \subseteq A$.

Now we prove the $\impliedby$ direction.

For the converse, assume that $B \subseteq A$.

We want to show that $A \cup B = A$. The equality holds if both $A \cup B \subseteq A$ and $A \subseteq A \cup B$. The inclusion $A \subseteq A \cup B$ follows immediately from the definition of $A \cup B$. So we really want to show that the condition $A \cup B \subseteq A$ holds, that is, that if $x \in A \cup B$ then $x \in A$.

Let $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in B$, then $x \in A$, because $B \subseteq A$ by assumption. Therefore $x \in A$, and so $A \cup B \subseteq A$.

Since $A \subseteq A \cup B$ always holds, it follows that $A \cup B = A$, so we have shown that $B \subseteq A \implies A \cup B = A$.

Finally, we can state our conclusion.

Hence $A \cup B = A \iff B \subseteq A$.

Exercise A113

Prove the following equivalences.

(a) n is even $\iff n + 8$ is even

(b) $A \subseteq A \cap B \iff A \subseteq B$.

Remember from Subsection 1.4 that an alternative way to express the equivalence $P \iff Q$ is to assert

$$P \implies Q \text{ and } (\text{not } P \implies \text{not } Q).$$

Thus the 'if' part of the equivalence – that is, $Q \implies P$ – can be proved by an argument that shows 'not $P \implies$ not Q'. This is sometimes convenient, as the next worked exercise shows.

Worked Exercise A57

Let n be a positive integer. Prove that

$$n \text{ is even} \iff n^3 \text{ is even}.$$

Solution

We start by proving the $\implies$ direction; that is, we assume that n is even and we want to deduce that n^3 is even.

Let n be an even integer. Then

$$n = 2k \text{ for some integer } k.$$

Hence

$$n^3 = (2k)^3 = 2 \times 4k^3.$$

Since $4k^3$ is an integer, this shows that n^3 is an even integer. Thus we have shown that if n is even, then n^3 is even.

We now need to prove the $\Longleftarrow$ direction; that is, we want to deduce that n is even from the assumption that n^3 is even. Writing $n^3 = 2k$ for some integer k does not seem to help in any obvious way to establish that n is even. Thus we try another approach: we assume that n is *not* even – that is, n is odd – and deduce that n^3 is odd. That is, we prove the contrapositive of the implication 'if n^3 is even, then n is even', which is equivalent to the implication.

Now assume that n is odd. Then

$$n = 2k + 1 \text{ for some integer } k.$$

Hence

$$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1.$$

Since $4k^3 + 6k^2 + 3k$ is an integer, this shows that n^3 is an odd integer.

Thus we have shown that if n is odd, then n^3 is odd, which is equivalent to the statement that n is even whenever n^3 is even.

Hence n is even $\iff$ n^3 is even, as required.

In the solution to Worked Exercise A57, the proof of the $\Longleftarrow$ direction is an example of *proof by contraposition*, a method that you will look at in detail in Subsection 3.2.

If you decide to prove an equivalence by using a sequence of $\iff$, as in Worked Exercise A55, you must be sure that its use is valid at each step; in other words, that both implications hold. This advice holds in general for proofs where it may be tempting to use a sequence of equivalences, rather than to look at each implication separately. The next worked exercise shows an example of a rash use of a sequence of equivalences.

Worked Exercise A58

Consider the following exercise.

> Let n be a positive integer. Prove that
>
> n is a multiple of 5 if and only if n^2 is a multiple of 5.

Explain why the proof below is incomplete.

Proof (incorrect!)

$$\begin{aligned} n \text{ is a multiple of } 5 &\iff n = 5k \text{ for some integer } k \\ &\iff n^2 = 25k^2 \text{ for some integer } k \\ &\iff n^2 = 5(5k^2) \text{ for some integer } k \\ &\iff n^2 \text{ is a multiple of } 5. \end{aligned}$$

■

Solution

The issue lies in the last equivalence in the sequence. While the implication

$$n^2 = 5(5k^2) \text{ for some integer } k \implies n^2 \text{ is a multiple of } 5$$

is clearly true, the converse implication

$$n^2 \text{ is a multiple of } 5 \implies n^2 = 5(5k^2) \text{ for some integer } k$$

requires further justification. The assumption 'n^2 is a multiple of 5' tells us that $n^2 = 5l$ for some integer l, but does not immediately warrant the conclusion that n^2 can be written in the form $5(5k^2)$. There is a difference between stating that a given number is a multiple of 5 and stating that it is a multiple of 5 written in the specific form $5(5k^2)$ for some integer k.

In the solution to Worked Exercise A58, separating the two implications to be proved would have helped avoid the issue with the incorrect proof. In Worked Exercise A70 in Section 3.2 you will see a proof of the implication

$$\text{if } n^2 \text{ is a multiple of } 5, \text{ then } n \text{ is a multiple of } 5$$

by *contraposition*, the method that we also used to prove the $\Longleftarrow$ direction in Worked Exercise A57. This implication can also be proved directly by using the Fundamental Theorem of Arithmetic and the fact that if a prime number p divides a product ab, then p divides a or p divides b.

Many theorems whose statement contains an equivalence have the form

If P, then (Q if and only if R).

or, equivalently,

Suppose P. Then (Q if and only if R).

In these cases, the assumption P holds throughout the proof. In addition, you assume Q when proving the implication 'if Q, then R', and you assume R when you prove the converse implication 'if R, then Q'. The Factor Theorem (Theorem A2 in Unit A2) has this form, and you already know enough to work through its proof.

This proof is longer and it may require more work to understand than the examples you have seen so far. However, it is a good example of how the ideas in this subsection, and in previous ones, appear in mathematical practice. If you get stuck with the details of the deductions, try to concentrate on the structure of the proof and come back to it when you have had more practice.

Theorem A2 Factor Theorem (in $\mathbb{R}$)

Let $p(x)$ be a real polynomial, and let $\alpha \in \mathbb{R}$. Then $p(\alpha) = 0$ if and only if $x - \alpha$ is a factor of $p(x)$.

Proof Throughout the proof, we assume that $p(x)$ is a real polynomial and that $\alpha \in \mathbb{R}$. Under these assumptions, we need to prove an equivalence. We tackle each implication separately, and we start with the 'if' direction. So we start by assuming that $x - \alpha$ is a factor of $p(x)$.

Assume first that $x - \alpha$ is a factor of $p(x)$, that is, assume that

$$p(x) = (x - \alpha)q(x)$$

for some real polynomial $q(x)$ whose degree is lower than the degree of $p(x)$. Then

$$p(\alpha) = (\alpha - \alpha)q(\alpha) = 0,$$

as required.

We now prove the 'only if' direction, so we assume that $p(\alpha) = 0$.

Now assume that $p(\alpha) = 0$, and let

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_n \neq 0$. Since $p(\alpha) = 0$, we have

$$\begin{aligned} p(x) &= p(x) - p(\alpha) \\ &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) \\ &\quad - (a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1 \alpha + a_0) \\ &= a_n(x^n - \alpha^n) + a_{n-1}(x^{n-1} - \alpha^{n-1}) + \cdots + a_1(x - \alpha), \end{aligned}$$

since the constant terms a_0 cancel.

Now, by Theorem A12 (the Geometric Series Identity), we know that $x - \alpha$ is a factor of each of the bracketed terms in this last expression, and so it is a factor of $p(x)$, as required.

This concludes our proof. ■

So far we have discussed proof only in the context of implications (and equivalences – though an equivalence is just two implications). Much of what we have said extends to proofs of other types of statements. A statement Q that is not an implication can be proved by building up a sequence of statements leading to Q in the way that we have seen for an

implication, except that there is no assumption P to be made at the start. Instead, the first statement in the sequence must be one that we know to be true from our previous mathematical knowledge.

In the next section we apply what you have learned so far to proving existential and universal statements.

2.3 Proving existential and universal statements

Statement 4 at the start of Subsection 1.1 is an example of a statement that is not an implication, nor an equivalence – it is an existential statement:

There is a real number x such that $\cos x = x$.

Existential statements can sometimes be proved by finding an object that satisfies the property in the statement.

Worked Exercise A59

Prove that there is a positive real number x such that $x < \sqrt{x}$.

Solution

Since x is assumed to be positive, the condition $x < \sqrt{x}$ is equivalent to $x^2 < x$, that is, to $x^2 - x < 0$. (Remember that the rules for rearranging inequalities are given in the module Handbook if you need to refer to them.)

Now

$$x^2 - x < 0 \iff x(x-1) < 0\,.$$

The product $x(x-1)$ is less than 0 if and only if one of x and $x-1$ is positive and the other is negative. Since x is assumed to be positive, any positive value of x such that $x < 1$ satisfies the inequality. So we can take, for example, $x = \frac{1}{9}$.

Let $x = \frac{1}{9}$. Then $\sqrt{x} = \frac{1}{3}$, and $\frac{1}{9} < \frac{1}{3}$.

Here is another example for you to try.

Exercise A114

Prove that there is an integer n such that $3^n > 9^n$.

However, constructing a mathematical object with a given property can be considerably harder than this, and even impossible: for example, we have no way to find an exact solution to the equation

$$\cos x = x,$$

and so we need an alternative way to prove Statement 4. We can note that the graphs of the functions $f(x) = \cos x$ and $g(x) = x$ intersect at least once, so the equation does have a solution. However, for a rigorous proof we need the Intermediate Value Theorem which is proved later in the module. In cases where an example is hard to find, other methods of proof should be tried. On the other hand, when an existential statement *can* be proved by explicitly describing a mathematical object, it is important to remember that *one* example suffices: it is bad style to give multiple examples.

To prove a *universal* statement about an infinite set, however, you always need to give a general argument. You have already seen many examples of this in this unit, since many of the statements you have met so far are universal, though the universal quantifier is often implicit. For example, the statement in Worked Exercise A50,

if n is odd, then n^2 is odd,

could be rephrased as

for all integers n, if n is odd, then n^2 is odd,

whilst the statement in Worked Exercise A52 contains an explicit universal quantifier:

for every integer n, the number $n^3 + 3n^2 + 2n$ is divisible by 6.

The proof of a universal statement is an argument, of the kind you have seen in previous examples in this unit, that applies to all the objects covered by the quantifier. It is important to remember that checking that the statement holds in particular instances, however many, does not constitute a proof of a universal statement about an infinite set.

2.4 Counterexamples

Proving that a statement is true can be difficult. However, you may suspect that a statement is false, and it can often (but not always!) be easier to deal with this situation, especially when the statement is universal.

For example, recall that statements of the form

$$P(x) \implies Q(x)$$

are in fact universal statements where the universal quantifier 'for all x' is omitted by convention. So the negation of $P(x) \implies Q(x)$ is

There is x such that $P(x)$ and not $Q(x)$.

Thus to prove that $P(x) \implies Q(x)$ is false, you just have to give *one* example of a case where the statement $P(x)$ is true but the statement $Q(x)$ is false. Such an example is called a **counterexample** to the implication. Here are two examples.

Worked Exercise A60

Show that each of the following implications about integers is false, by giving counterexamples.

(a) If the product mn is a multiple of 4, then both m and n are multiples of 2.

(b) If n is prime, then $2^n - 1$ is prime.

Solution

(a) Taking $m = 4$ and $n = 1$ provides a counterexample because then $mn = 4$, which is a multiple of 4, but n is not a multiple of 2. Hence the implication is false.

(b) The number 11 is a counterexample because 11 is prime but $2^{11} - 1 = 2047$, which is not prime since $2047 = 23 \times 89$. Hence the implication is false.

Remember that just *one* counterexample is sufficient. For example, you can show that the statement

if $x^2 > 4$, then $x > 2$

is false by considering the value $x = -3$. There is no need to show that every number x less than -2 is a counterexample, even though this is the case.

There is no general method for finding counterexamples. For some statements, such as the statement in Worked Exercise A60(a), a little thought about the statement should suggest a suitable counterexample. For other statements, the quickest method may just be to try out different values for the variable (or variables) until you find a counterexample. For example, for the statement in Worked Exercise A60(b) we can repeatedly choose a prime number n, calculate $2^n - 1$ and check whether it is prime.

In order to carry out this procedure, we need a method for checking whether a given number m is prime. We could simply check whether m is divisible by each of the integers between 2 and $m - 1$ inclusive, but this involves a large amount of calculation even for fairly small integers m. We can significantly reduce the amount of calculation needed by using the following fact, which holds for any integer $m \geq 2$:

If m is not divisible by any of the primes less than or equal to $\sqrt{m}$, then m is a prime number.

You will be asked to prove this statement in Subsection 3.2. Here is an example of its use.

Worked Exercise A61

Show that 127 is a prime number.

Solution

We have $\sqrt{127} = 11.3$ to one decimal place, so the primes less than or equal to $\sqrt{127}$ are $2, 3, 5, 7$ and 11. Dividing 127 by each of these in turn gives a non-integer answer in each case, so 127 is prime.

Exercise A115

Give a counterexample to disprove each of the following implications.

(a) If $m + n$ is even, then both m and n are even.

(b) If $x < 2$, then $(x^2 - 2)^2 < 4$.

(c) If n is a positive integer, then $4^n + 1$ is prime.

As with implications, you may sometimes suspect that an equivalence is false. To prove that an equivalence $P \iff Q$ is false, you have to show that at least one of the implications $P \implies Q$ and $Q \implies P$ is false, which you can do by providing a counterexample; that is, you need a case where one of P or Q is true, and the other is false.

Exercise A116

Show that the equivalence

$$x^2 = 9 \iff x = 3$$

is false.

2.5 Proof by induction

Mathematical induction is a powerful method of proof that is particularly useful for proving statements involving integers, but also has wider applications.

The great French mathematician Henri Poincaré (1854–1912) described proof by mathematical induction as 'mathematical reasoning par excellence'.

Consider, for example, Statement 3 in our list at the beginning of Subsection 1.1:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 \text{ for each positive integer } n.$$

Let us denote the variable proposition

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

by $P(n)$. It is easy to check that $P(n)$ is true for small values of n; for example

$$1 = 1^2,$$
$$1 + 3 = 4 = 2^2,$$
$$1 + 3 + 5 = 9 = 3^2,$$

so certainly $P(1)$, $P(2)$ and $P(3)$ are all true. But how can we prove that $P(n)$ is true for all positive integers n?

The method of induction works like this. Suppose that we wish to prove that a statement $P(n)$, such as the one above, is true for all positive integers n. Now suppose that we have proved that the following two statements are true.

1. $P(1)$.
2. If $P(k)$ is true, then so is $P(k + 1)$, for $k = 1, 2, \ldots$.

Let us consider what we can deduce from this. Certainly $P(1)$ is true, because that is statement 1. Also $P(2)$ is true because, by statement 2, if $P(1)$ is true, then so is $P(2)$. Similarly, by statement 2, $P(3)$ is true since $P(2)$ is. Since this process goes on for ever, we can deduce that $P(n)$ is true for all positive integers n. We thus have the following method.

Principle of Mathematical Induction

To prove that a statement $P(n)$ is true for $n = 1, 2, \ldots$:

1. show that $P(1)$ is true
2. show that the implication $P(k) \implies P(k + 1)$ is true for $k = 1, 2, \ldots$.

Mathematical induction is often compared to pushing over a line of dominoes – this is illustrated in Figure 2. Imagine a (possibly infinite!) line of dominoes set up in such a way that if any one domino falls then the next domino in line will fall too – this is analogous to step 2 above. Now imagine pushing over the first domino – this is analogous to step 1. The result is that *all* the dominoes fall!

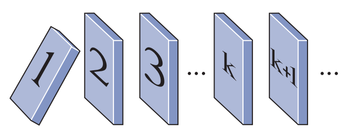


Figure 2 Toppling dominoes

Augustus De Morgan

Although indications of the method of mathematical induction can be found earlier, the first satisfactory formulations of the method are due to Pierre de Fermat (1601?–1665) in his work on number theory of 1630 (although not published until 1670) and Blaise Pascal (1623–1662) in a book on arithmetical triangles of 1654.

The term *mathematical induction* was introduced by the British mathematician Augustus De Morgan (1806–1871) in 1838 in an article he wrote for the *Penny Cyclopedia*.

In the next worked exercise we apply mathematical induction to prove the statement mentioned at the beginning of this subsection.

Worked Exercise A62

Prove that

$$1 + 3 + \cdots + (2n-1) = n^2, \text{ for } n = 1, 2, \ldots.$$

Solution

Write out $P(n)$.

Let $P(n)$ be the statement $1 + 3 + \cdots + (2n-1) = n^2$.

Next, carry out step 1, that is, check that $P(1)$ holds.

$P(1)$ is true because $1 = 1^2$.

Now proceed with step 2. State the assumption, $P(k)$.

Now let $k \geq 1$, and assume that $P(k)$ is true; that is,

$$1 + 3 + \cdots + (2k-1) = k^2.$$

State the desired conclusion, $P(k+1)$. The final term on the left-hand side of $P(k+1)$ is $2(k+1) - 1 = 2k+1$.

We wish to deduce that $P(k+1)$ is true; that is,

$$1 + 3 + \cdots + (2k-1) + (2k+1) = (k+1)^2.$$

Now prove that $P(k) \implies P(k+1)$. It should help to start with the left-hand side of the equality in $P(k+1)$ and rearrange it in such a way that $P(k)$ can be used.

Now

$$\begin{aligned} 1 + 3 + \cdots + (2k-1) + (2k+1) &= (1 + 3 + \cdots + (2k-1)) + (2k+1) \\ &= k^2 + (2k+1) \quad (\text{by } P(k)) \\ &= (k+1)^2. \end{aligned}$$

This proves that $P(k) \implies P(k+1)$, so we write out our conclusions.

Thus we have shown that

$$P(k) \implies P(k+1), \text{ for } k = 1, 2, \ldots.$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$.

Exercise A117

Prove each of the following statements by mathematical induction.

(a) $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$, for $n = 1, 2, \ldots$.

(b) $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$, for $n = 1, 2, \ldots$.

In the next worked exercise the argument used to prove $P(k+1)$ from $P(k)$ involves a more sophisticated algebraic manipulation than in Worked Exercise A62 and Exercise A117.

Worked Exercise A63

Prove that $2^{3n+1} + 5$ is a multiple of 7, for $n = 1, 2, \ldots$.

Solution

Let $P(n)$ be the statement

$2^{3n+1} + 5$ is a multiple of 7.

$P(1)$ is true because $2^{3\times1+1} + 5 = 2^4 + 5 = 21 = 3 \times 7$.

Now let $k \geq 1$, and assume that $P(k)$ is true; that is,

$2^{3k+1} + 5$ is a multiple of 7.

We wish to deduce that $P(k+1)$ is true; that is,

$2^{3(k+1)+1} + 5 = 2^{3k+4} + 5$ is a multiple of 7.

We need an algebraic manipulation that creates the subexpression 2^{3k+1} on the right-hand side, so that we can use $P(k)$. Now, the exponent of 2 in $P(k+1)$ is $3k+4$. Note that $3k+4 = 3 + (3k+1)$, and $3k+1$ is the exponent of 2 in $P(k)$.

Now

$$\begin{aligned} 2^{3k+4} + 5 &= 2^3 2^{3k+1} + 5 \\ &= 8 \times 2^{3k+1} + 5 \\ &= 7 \times 2^{3k+1} + 2^{3k+1} + 5. \end{aligned}$$

The first term here is a multiple of 7, and $2^{3k+1} + 5$ is a multiple of 7, by $P(k)$. Therefore $2^{3k+4} + 5$ is a multiple of 7. Thus we have shown that

$$P(k) \implies P(k+1), \text{ for } k = 1, 2, \ldots.$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$.

Mathematical induction can be adapted to deal with situations that differ a little from the standard one. For example, if a statement $P(n)$ is not true for $n = 1$ but we wish to prove that it is true for $n = 2, 3, \ldots$, then we can do this by following the usual method, except that in step 1 we prove that $P(2)$, rather than $P(1)$, is true. This is analogous to pushing over the second domino in the line: the result is that all the dominoes except the first fall!

Also, in step 2 we have to show that $P(k) \implies P(k+1)$ for $k = 2, 3 \ldots$, rather than for $k = 1, 2, \ldots$. In the next worked exercise we prove that a statement is true for $n = 7, 8, \ldots$.

Worked Exercise A64

Prove that $3^n < n!$ for all $n \geq 7$.

Solution

Let $P(n)$ be the statement '$3^n < n!$'.

We are told to prove the statement for all $n \geq 7$, so we consider $P(7)$.

$P(7)$ is true because $3^7 = 2187 < 5040 = 7!$.

Now let $k \geq 7$, and assume that $P(k)$ is true; that is,

$$3^k < k!.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$3^{k+1} < (k+1)!.$$

Now

$$\begin{aligned} 3^{k+1} &= 3 \times 3^k \\ &< 3 \times k! \quad (\text{by } P(k)) \\ &< (k+1)k! \quad (\text{because } k \geq 7, \text{ and hence } k+1 \geq 8 > 3) \\ &= (k+1)!. \end{aligned}$$

The conclusion $P(k) \implies P(k+1)$ holds for all $k \geq 7$.

Hence $P(k) \implies P(k+1)$, for $k = 7, 8, \ldots$.

Hence, by mathematical induction, $P(n)$ is true, for $n = 7, 8, \ldots$.

$P(n)$ happens to be false for $n = 1, 2, \ldots, 6$ in Worked Exercise A64 (you can check this if you like). However, the proof does not require any mention of this fact.

Exercise A118

Prove each of the following statements by mathematical induction.

(a) $4^{2n-3} + 1$ is a multiple of 5, for $n = 2, 3, \ldots$.

(b) $5^n < n!$ for all $n \geq 12$.

Proof by induction is also useful in many cases where the statement to be proved does not concern a property of the integers. You have already met at least one theorem that can be proved in this way: Theorem A3 in Unit A2 concerns all real polynomials that have as many distinct roots as their degree. The general statement can be proved by showing that it holds for all real polynomials of degree n with n distinct roots, for each $n \in \mathbb{N}$. Below you will see that the proof applies the Principle of Mathematical Induction to the degree n.

This proof, rather like the proof of the Factor Theorem in Subsection 2.2, is more advanced than the induction proofs you have seen so far in this subsection. Similar advice applies here as for the proof of the Factor Theorem: if the details of the deductions are not clear to you, try to concentrate on the structure of the proof, in particular on how the Principle of Mathematical Induction is used, and if necessary come back to the proof at a later stage.

Theorem A3

Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a real polynomial, and suppose that $p(x)$ has n distinct real roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n).$$

Proof If we show that the result holds for all polynomials of degree n with n distinct roots, for $n \in \mathbb{N}$, then we have proved the general statement in the theorem.

We argue by induction on the degree n. Let $P(n)$ be the statement

> If $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a real polynomial with distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, then
> $$p(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n).$$

Step 1 is to show that the statement holds for all polynomials of degree 1 with one real root; that is, we want to show that all polynomials of the form $a_1 x + x_0$ can be written in the form $a_1(x - \alpha_1)$, where α_1 is a root.

$P(1)$ is true since if $p(x) = a_1x + a_0$ (where $a_1 \neq 0$) is a real polynomial with root α_1, then $p(\alpha_1) = 0$. So

$$a_1\alpha_1 + a_0 = 0,$$

and so $a_0 = -a_1\alpha_1$. Thus

$$p(x) = a_1x - a_1\alpha_1 = a_1(x - \alpha_1),$$

as required.

In order to carry out step 2, we assume that the theorem holds for all polynomials of degree k with k distinct real roots, and we want to deduce that it holds for all polynomials of degree $k+1$.

Suppose that $P(k)$ is true; that is, suppose that all polynomials of degree k with k distinct real roots have a factorisation of the form

$$a_k(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_k)$$

where $\alpha_1, \ldots, \alpha_k$ are the roots.

We wish to deduce that $P(k+1)$ holds; that is, all polynomials of degree $k+1$ with $k+1$ distinct real roots have a factorisation of the form

$$a_{k+1}(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_{k+1})$$

where $\alpha_1, \ldots, \alpha_{k+1}$ are the roots.

So let

$$q(x) = a_{k+1}x^{k+1} + a_kx^k + \cdots + a_1x + a_0,$$

where $a_{k+1} \neq 0$, be a polynomial of degree $k+1$ with $k+1$ distinct real roots. Let α_{k+1} be a root of $q(x)$. By the Factor Theorem, we have that $x - \alpha_{k+1}$ is a factor of $q(x)$, so

$$q(x) = (x - \alpha_{k+1})\,r(x),$$

where $r(x)$ is a polynomial of degree k. Moreover, the coefficient of x^k in $r(x)$ must be a_{k+1}.

In order to apply $P(k)$ to $r(x)$, we also need to show that $r(x)$ has k distinct roots.

Now let α be a root of $q(x)$ other than α_{k+1}. Then $q(\alpha) = 0$, that is,

$$(\alpha - \alpha_{k+1})\,r(\alpha) = 0.$$

Since $\alpha \neq \alpha_{k+1}$, we have $\alpha - \alpha_{k+1} \neq 0$, and so we must have $r(\alpha) = 0$. Thus α is a root of $r(x)$. Since $q(x)$ has $k+1$ distinct real roots, including α_{k+1}, it follows that $r(x)$ has k distinct real roots.

Since $r(x)$ is a polynomial of degree k with k distinct roots, we can apply $P(k)$.

By $P(k)$, the polynomial $r(x)$ has a factorisation

$$r(x) = a_{k+1}(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_k).$$

Thus

$$\begin{aligned} q(x) &= (x-\alpha_{k+1})\,a_{k+1}(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k) \\ &= a_{k+1}(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)(x-\alpha_{k+1}). \end{aligned}$$

Therefore $q(x)$ has a factorisation of the required form. Thus we have shown that $P(k) \implies P(k+1)$, for $k = 1, 2, \ldots$. Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$. ■

The next exercise asks you to use induction to give a rigorous proof of the powers property of congruences that appears in Theorem A10 in Unit A2 (an informal proof was given in Unit A2). Recall that two integers a and b are congruent modulo n, written $a \equiv b \pmod{n}$, if $a - b$ is a multiple of n. In the proof, you will need to use the multiplication property of congruences, which was also part of Theorem A10:

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Exercise A119

Let a, b and n be integers. Use the Principle of Mathematical Induction and the multiplication property of congruences to prove that

if $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$,

for $m = 1, 2, \ldots$.

Hint: Since you need to prove this statement for $m = 1, 2, \ldots$, call the statement $P(m)$ and use induction on m.

Finally in this section, here is some advice to consolidate what you have learned about induction proofs. When you write a proof by induction make sure that you clearly identify the statement to be proved, $P(n)$, and structure your proof as follows:

- prove that $P(1)$ holds (or $P(n_0)$ for some initial $n_0 \neq 1$)
- write down $P(k)$ and assume that it holds for a general k
- state that we need to deduce $P(k+1)$, and write down $P(k+1)$
- deduce $P(k+1)$ from $P(k)$
- conclude that $P(n)$ holds for all natural numbers n (or for all $n \geq n_0$ where appropriate).

If you are unsure about your proof, review it and check that it follows this structure; in particular, check that $P(1)$ (or $P(n_0)$ where appropriate) is proved correctly, and that you have used $P(k)$ in the proof of $P(k+1)$.

Not all the proofs by induction that you will meet in the module materials, or in other textbooks, will match this format exactly, but this advice should help you *write* your own induction proofs. Below is an example of what can go wrong if you do not follow this template.

Worked Exercise A65

Consider the statement

$$2^1 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2 \text{ for } n = 1, 2, \ldots.$$

Explain why the proof below is not a correct proof by induction, and write a correct proof.

Proof (incorrect!) Let $P(n)$ be the statement

$$2^1 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2.$$

$P(1)$ is true because $2^1 = 2^{1+1} - 2 = 2^2 - 2$.

Now let $k \geq 1$. Assume $P(k)$; that is, assume that

$$2^1 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 2.$$

We wish to deduce that $P(k+1)$ is true; that is

$$2^1 + 2^2 + 2^3 + \cdots + 2^{k+1} = 2^{k+2} - 2.$$

Dividing both sides of $P(k+1)$ by 2 gives

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$$

hence

$$2 + 2^2 + \cdots + 2^k = 2^{k+1} - 2 \text{ by rearranging.}$$

Since we have obtained $P(k)$, which we assume is true, we know that $P(k+1)$ is true.

Therefore $P(n)$ is true for $n = 1, 2, \ldots$ by mathematical induction. ■

Solution

Step 1 is correct, as is step 2 up to the statement of $P(k+1)$. However, step 2 is a deduction of $P(k)$ from $P(k+1)$, rather than the required proof that $P(k)$ implies $P(k+1)$. The fact that $P(k+1)$ implies a statement that we assume to be true does not constitute a proof of $P(k+1)$.

A correct version of step 2 is as follows.

Assume $P(k)$; that is, assume that

$$2^1 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 2.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$2^1 + 2^2 + 2^3 + \cdots + 2^{k+1} = 2^{k+2} - 2.$$

We have

$$\begin{aligned}2^1 + 2^2 + \cdots + 2^k + 2^{k+1} &= (2^1 + 2^2 + 2^3 + \cdots + 2^k) + 2^{k+1} \\ &= 2^{k+1} - 2 + 2^{k+1} \quad (\text{by } P(k)) \\ &= 2 \times 2^{k+1} - 2 = 2^{k+2} - 2.\end{aligned}$$

Thus $P(k) \implies P(k+1)$, for $k = 1, 2, \ldots$. Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$.

Exercise A120

Consider the statement

$$2^n + 1 \leq 3^n, \quad \text{for } n = 1, 2, \ldots.$$

Explain why the following proof is not a correct induction argument, and give a correct proof.

Proof (incorrect!) Let $P(n)$ be the statement $2^n + 1 \leq 3^n$.

$P(1)$ is true since $2^1 + 1 = 3$.

Assume $P(k)$; that is, assume that $2^k + 1 \leq 3^k$.

We wish to deduce that $P(k+1)$ is true; that is

$$2^{k+1} + 1 \leq 3^{k+1}.$$

We have

$$\begin{aligned}2^k + 1 &\leq 2(2^k + 1) \\ &= 2 \times 3^k \quad (\text{by } P(k)).\end{aligned}$$

Since $2 \times 3^k \leq 3 \times 3^k = 3^{k+1}$, we have that $P(k+1)$ holds.

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$. ■

3 Indirect proof

The proof methods that you will meet in this section are indirect in that they do not show directly that the statement to be proved is true. Instead, a proof by *contradiction* assumes that the statement to be proved is false and deduces a statement that cannot be true at the same time as some of the assumptions (or some other true mathematical statement), and in a proof by *contraposition* the contrapositive is proved, rather than the original implication.

3.1 Proof by contradiction

Sometimes a useful approach to proving a statement is to ask yourself, 'Well, what if the statement were false?'. Consider the following example.

Worked Exercise A66

Prove that there is no positive real number a such that

$$a + \frac{1}{a} < 2.$$

Solution

Suppose that there *is* a positive real number a such that

$$a + \frac{1}{a} < 2.$$

Then, since a is positive, we have

$$a\left(a + \frac{1}{a}\right) < 2a,$$

which, on multiplying out and rearranging, gives

$$a^2 - 2a + 1 < 0;$$

that is,

$$(a-1)^2 < 0.$$

But this is impossible, since the square of every real number is greater than or equal to zero. Hence we can conclude that there is no such real number a.

The proof above is an example of **proof by contradiction**. The idea is that if we wish to prove that a statement Q is true, then we begin by *assuming* that Q is *false*. We then attempt to deduce, using the method of a sequence of statements that you saw in Subsection 2.1, a statement that is definitely false, which in this context is called a **contradiction**. If this can be achieved, then since everything about our argument is valid except possibly the assumption that Q is false, and yet we have deduced a contradiction, we can conclude that the assumption is in fact false – in other words, Q is true.

You have already met this kind of proof: the proof of Theorem A1 given in Unit A2 is a proof by contradiction. It is repeated below, with further explanation of the thinking behind it.

Theorem A1

There is no rational number x such that $x^2 = 2$.

Proof We assume that x is a rational number such that $x^2 = 2$ and aim for a contradiction.

Suppose for a contradiction that there is a rational number x such that $x^2 = 2$. Since x is rational, we can write $x = p/q$, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. By replacing p/q by an equivalent fraction in lowest terms, if necessary, we may assume that the highest common factor of p and q is 1 (that is, that p and q are coprime). The equation $x^2 = 2$ now becomes

$$\frac{p^2}{q^2} = 2,$$

so

$$p^2 = 2q^2. \tag{1}$$

Therefore p^2 is even, which implies that p is even (we know that if p were odd, then p^2 would also be odd). So we can write $p = 2r$, where r is an integer, and equation (1) becomes

$$(2r)^2 = 2q^2.$$

Therefore we have

$$q^2 = 2r^2,$$

that is, q^2 is even. By a similar argument to that for p, we deduce that q is even.

If both p and q are even, then they are not coprime.

Since p and q are both even, 2 is a common factor of p and q. But we assumed p/q to be a fraction in its lowest terms, so this is a contradiction.

Since we have obtained a contradiction, our assumption that x is a rational number such that $x^2 = 2$ must be false.

Therefore no rational number x exists such that $x^2 = 2$. ■

Exercise A121

Show that there is no rational number x such that $x^3 = 2$.

The English mathematician G. H. Hardy (1877–1947) described proof by contradiction as 'one of a mathematician's finest weapons'. One of his favourite examples was a proof by contradiction of the existence of infinitely many primes. A version of the proof is given next. A proof of this result was originally given by Euclid in about 300 BCE, and it was essentially a proof by contradiction.

G. H. Hardy

Theorem A14

There are infinitely many prime numbers.

Proof Suppose that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Consider the integer

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

This integer is greater than each of the primes $p_1, p_2, \ldots, p_n$, so by our assumption it is not prime.

We can use the Fundamental Theorem of Arithmetic (Theorem A13) to deduce that N has a prime factor.

Now N has a prime factor, p say, by the Fundamental Theorem of Arithmetic. But p cannot be any of the primes $p_1, p_2, \ldots, p_n$, since dividing any one of these into N leaves the remainder 1. Thus, p is a prime other than $p_1, p_2, \ldots, p_n$. This is a contradiction, so our assumption that there are only finitely many primes must be false. It follows that there are infinitely many primes. ■

In the next exercise you can practise proof by contradiction for statements that are similar to that in Worked Exercise A66, in that they assert the non-existence of numbers with a certain property.

Exercise A122

Use proof by contradiction to prove each of the following statements.

(a) There are no real numbers a and b with $ab > \frac{1}{2}(a^2 + b^2)$.

(b) There are no integers m and n with $5m + 15n = 357$.

The next worked exercise uses proof by contradiction to prove a general statement about sets.

Worked Exercise A67

Prove that, for any two sets A and B,

$$A \cap (B - A) = \varnothing.$$

Solution

Suppose for a contradiction that $A \cap (B - A) \neq \varnothing$. Then there is an element, x, such that $x \in A \cap (B - A)$; that is, there is an x such that $x \in A$ and $x \in B - A$. But then, since $x \in B - A$, we have that $x \notin A$, which is a contradiction.

Therefore $A \cap (B - A) = \varnothing$, as required.

Proof by contradiction can sometimes be used to prove an implication. To prove an implication $P \implies Q$ by contradiction, you should begin by assuming that the implication is false, hoping for a contradiction. That is, you should assume that P is true and Q is false. If under these assumptions you can deduce a contradiction, then you can conclude that if P is true, then Q must also be true, which is the required implication. Here is an example.

Worked Exercise A68

Prove that if $n = ab$ where $n > 0$, then at least one of a and b is less than or equal to $\sqrt{n}$.

Solution

Suppose that $n = ab$ where $n > 0$.

We start by assuming that the implication is false, which means that both a and b are greater than $\sqrt{n}$. We then try to deduce a contradiction.

Suppose also that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then

$$n = ab > (\sqrt{n})(\sqrt{n}) = n;$$

that is, $n > n$. This contradiction shows that the supposition that $a > \sqrt{n}$ and $b > \sqrt{n}$ must be false; that is, at least one of a and b is less than or equal to $\sqrt{n}$.

Exercise A123

Use proof by contradiction to prove that if $n = a + 2b$, where a and b are positive real numbers, then $a \geq \frac{1}{2}n$ or $b \geq \frac{1}{4}n$.

As a final example that applies what you have learned in this subsection to a result that you have already met, we give below a formal proof of Theorem A11 from Unit A2, restated as an equivalence. One of the implications is proved by contradiction.

The usual advice applies that if the details of the proof are not all clear, for now you should concentrate on the structure of the proof, in particular on how the 'only if' direction is proved by contradiction.

Theorem A11

Let n and a be positive integers, with a in $\mathbb{Z}_n$. Then a has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a and n are coprime.

Proof We assume that n is a positive integer and $a \in \mathbb{Z}_n$. We start by proving the 'only if' direction. We assume that a has a multiplicative inverse in $\mathbb{Z}_n$ and we want to deduce that a and n are coprime. We argue by contradiction.

Suppose that a has a multiplicative inverse in $\mathbb{Z}_n$, and assume for a contradiction that a and n are not coprime, that is, that a and n have a common factor $d > 1$.

Let b be the multiplicative inverse of a in $\mathbb{Z}_n$; then $b \times_n a = 1$, and so

$$ba = kn + 1$$

for some integer k, and therefore $ba - kn = 1$.

Any common factor of a and n is also a common factor of ba and kn, and therefore of $ba - kn$.

Since d is a common factor of a and n, we have that d divides $ba - kn$. But this is a contradiction, since $ba - kn = 1$ and $d > 1$.

The assumption that a and b are not coprime leads to a contradiction, so we conclude that a and b are coprime.

Therefore a and b are coprime.

We now prove the 'if' direction in the equivalence, so we start by assuming that a and n are coprime.

Now let a and n be coprime.

For this direction of the proof we use Euclid's Algorithm, a method for finding the highest common factor of two positive integers that you met in Unit A2. By the Division Theorem, quoted in Subsection 1.3, we know that there are unique integers q_1 and r_1 such that

$$n = q_1 a + r_1, \quad \text{with } 0 \leq r_1 < a.$$

Euclid's Algorithm proceeds by applying the Division Theorem again to the remainder r_1, and then successively repeating this step.

We apply Euclid's Algorithm. From one step of the algorithm to the next, the remainder decreases by at least 1, so it must eventually reach 0. We have

$$\begin{aligned}
n &= q_1 a + r_1 & \qquad 0 &< r_1 < a\\
a &= q_2 r_1 + r_2 & 0 &< r_2 < r_1\\
r_1 &= q_3 r_2 + r_3 & 0 &< r_3 < r_2\\
&\ \ \vdots & &\ \ \vdots\\
r_{m-2} &= q_m r_{m-1} + r_m & 0 &< r_m < r_{m-1}\\
r_{m-1} &= q_{m+1} r_m + 0. & &
\end{aligned}$$

The final equation shows that r_m is a factor of r_{m-1}.

Since r_m is a factor of r_{m-1}, it is also a factor of $q_m r_{m-1}$, and therefore of $q_m r_{m-1} + r_m$. Hence r_m is also a factor of r_{m-2}, and so on up the list.

Therefore the penultimate equation shows that r_m is a factor of r_{m-2}, and so on. In this way, we find that r_m is a factor of all the remainders $r_m, r_{m-1}, \ldots, r_1$, and so of both a and n.

Since a and n are coprime by assumption, their only common factor is 1.

Since we assumed that a and n are coprime, we deduce that $r_m = 1$.

Therefore the penultimate equation gives

$$1 = r_{m-2} - q_m r_{m-1}.$$

By backwards substitution we find that there are integers k and d such that $1 = kn + da$. Hence $da = -kn + 1$, that is, $d \times_n a = 1$.

If $d \in \mathbb{Z}_n$, then d is a multiplicative inverse of a in $\mathbb{Z}_n$.

If $d \notin \mathbb{Z}_n$, we have $d \equiv b \pmod{n}$ for some $b \in \mathbb{Z}_n$, where $b \neq 0$ and $b \times_n a = 1$. Hence b is a multiplicative inverse of a in $\mathbb{Z}_n$.

Therefore in either case a has a multiplicative inverse in $\mathbb{Z}_n$, as required. ■

3.2 Proof by contraposition

Recall that the contrapositive of the implication 'if P, then Q' is 'if not Q, then not P', where 'not P' and 'not Q' denote the negations of the statements P and Q, respectively.

Since an implication and its contrapositive are equivalent, if you have proved one, then you have proved the other. Sometimes the easiest way to prove an implication is to prove its contrapositive instead. This is called **proof by contraposition**. Here is an example. The proof makes use of the following identity, which is a special case of the Geometric Series Identity (Theorem A12) that you met at the beginning of Section 2: for any real number x and any positive integer n, we have

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1). \tag{2}$$

Worked Exercise A69

Prove the following implication about positive integers n:

if $2^n - 1$ is prime, then n is prime.

Solution

We prove the contrapositive of the implication, which is

if n is not prime, then $2^n - 1$ is not prime.

Suppose that n is a positive integer that is not prime.

We consider two cases separately: the cases $n = 1$ and $n > 1$. Splitting into separate cases is sometimes an effective way to proceed in a proof.

If $n = 1$, then $2^n - 1 = 2 - 1 = 1$, which is not prime.

If $n > 1$, then since n is not prime by our assumption, we can write $n = ab$, where $1 < a,\ b < n$. Hence

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1)((2^a)^{b-1} + \cdots + 2^a + 1), \end{aligned}$$

where the last line follows from equation (2) by taking $x = 2^a$ and $n = b$.

Now $2^a - 1 > 1$ since $a > 1$, and also $(2^a)^{b-1} + \cdots + 2^a + 1 > 1$ since both a and b are greater than 1. Hence $2^n - 1$ is not prime. We have thus proved the required contrapositive implication in both the cases $n = 1$ and $n > 1$. Hence the original implication is also true.

When proving results about integers, proof by contraposition is especially useful when the conclusion has the form 'n is even', or 'n is odd', or a combination of statements of this kind. Below is a different example that in fact gives a proof by contraposition of the missing implication in Worked Exercise A58 in Subsection 2.2.

Recall from Subsection 3.2 of Unit A2 that for integers a, b and n, $a \equiv b \pmod{n}$ if (and only if) a and b have the same remainder on division by n.

Worked Exercise A70

Prove the 'if' direction of the statement in Worked Exercise A58; that is, prove that, if n is a positive integer,

if n^2 is a multiple of 5, then n is a multiple of 5.

Solution

We have seen in Worked Exercise A58 that the assumption 'n^2 is a multiple of 5' does not help us reach the conclusion in any obvious way, so we try proving the contrapositive.

We prove the contrapositive implication, which is

if n is not a multiple of 5, then n^2 is not a multiple of 5.

Suppose that n is not a multiple of 5.

Then, by the Division Theorem, n can be written as one of

$$5k + 1 \text{ or } 5k + 2 \text{ or } 5k + 3 \text{ or } 5k + 4,$$

for some integer k, and so one of the following holds:

$$n \equiv 1 \pmod{5} \text{ or } n \equiv 2 \pmod{5} \text{ or } n \equiv 3 \pmod{5} \text{ or } n \equiv 4 \pmod{5}.$$

We consider each of these cases.

We use the powers property of congruences which you proved in Exercise A119. For congruences modulo 5 it follows from this result that if $a \equiv b \pmod{5}$, then $a^2 \equiv b^2 \pmod{5}$.

If $n \equiv 1 \pmod{5}$, then $n^2 \equiv 1 \pmod{5}$. If $n \equiv 2 \pmod{5}$, then $n^2 \equiv 2^2 \equiv 4 \pmod{5}$. Similarly, if $n \equiv 3 \pmod{5}$, then $n^2 \equiv 9 \equiv 4 \pmod{5}$, and if $n \equiv 4 \pmod{5}$, then $n^2 \equiv 16 \equiv 1 \pmod{5}$.

These cases cover all the possibilities for n^2, and in each case the remainder on dividing n^2 by 5 is not zero.

Therefore n^2 is not a multiple of 5, as required.

Since the contrapositive is true, the original implication is also true.

Exercise A124

Use proof by contraposition to prove each of the following statements about integers m and n.

(a) If $n^3 + 2n + 1$ is even, then n is odd.

(b) If mn is odd, then both m and n are odd.

(c) If an integer $n > 1$ is not divisible by any of the primes less than or equal to $\sqrt{n}$, then n is a prime number.

Hint: Use the result of Worked Exercise A68.

The next worked exercise involves a statement about sets that can be proved rather neatly by contraposition.

Worked Exercise A71

Prove that, for any sets A and B,

$$\text{if } (A - B) \cup (B - A) = A \cup B, \text{ then } A \cap B = \varnothing.$$

Solution

The hypothesis of the implication that we are required to prove is a more complex statement than the conclusion. It might be easier to prove the contrapositive since the negation of the conclusion, '$A \cap B \neq \varnothing$', is a clearer hypothesis that is easier to understand.

We prove the contrapositive implication, which is

$$\text{if } A \cap B \neq \varnothing, \text{ then } (A - B) \cup (B - A) \neq A \cup B.$$

Suppose that $A \cap B \neq \varnothing$. Then there is an element x such that $x \in A$ and $x \in B$, so $x \in A \cup B$.

However, $x \notin A - B$, because $x \in B$. Similarly, $x \notin B - A$. Therefore $x \notin (A - B) \cup (B - A)$. So x is an element of $A \cup B$ that is not in $(A - B) \cup (B - A)$. Hence

$$(A - B) \cup (B - A) \neq A \cup B,$$

as required.

The contrapositive is true, therefore the original statement is also true.

Exercise A125

Let A and B be sets. Prove that

$$\text{if } A \subseteq B, \text{ then } A - B = \varnothing.$$

The final exercise in this subsection asks you to read critically an attempted proof by contraposition.

Exercise A126

Consider the statement

$$\text{if } n^3 + 3 \text{ is even, then } n \text{ is odd.}$$

Explain why the argument below is not a correct proof of this statement, and give a correct proof.

Proof (incorrect!) We prove the contrapositive, that is

if n is odd, then $n^3 + 3$ is even.

Assume n is odd. Then $n = 2k + 1$ for some integer k, and so

$$\begin{aligned} n^3 + 3 &= (2k+1)^3 + 3 \\ &= 8k^3 + 12k^2 + 6k + 1 + 3 \\ &= 8k^3 + 12k^2 + 6k + 4 \\ &= 2(4k^3 + 6k^2 + 3k + 2). \end{aligned}$$

This shows that $n^3 + 3$ is even, as required. ■

The exercise above is an example of a common pitfall when trying to prove a statement by contraposition, that is, a mistake in finding the contrapositive.

You may have found some of the ideas so far in this unit difficult to get used to; this is to be expected since reading and understanding mathematics, and writing mathematics clearly and accurately, can both be difficult at first. Your skills will improve as you gain experience. To accelerate this improvement, you should, when reading mathematics, try to make sure that you gain a clear understanding of exactly what each statement asserts. When writing mathematics, you should try to be as clear and accurate as you can. Include enough detail to make the argument clear, but omit any statements that are not necessary to reach the required conclusion. A good check is to read over your work and ask yourself whether you would be able to follow what you have written in six months' time, when you have forgotten the thoughts and rough work that led to it. Use the solutions to the exercises and worked exercises in the module as models for good mathematical writing.

You may find it helpful to revisit parts of Sections 1, 2 and 3 later in your study of the module.

4 Equivalence relations

In this section you can apply many of the ideas about careful, logical thinking and proof that you have learned in the previous sections of this unit to a new topic in which this approach is needed. This topic is the important one of *equivalence relations.* Equivalence relations occur throughout mathematics, and are particularly important in the group theory units of this module.

4.1 What is an equivalence relation?

As you would expect, an *equivalence relation* is a special type of relation, so we will start by looking at what is meant by a *relation*.

In everyday life we often work with *relations* between objects. For example, *is a child of* is a relation between people: we might say 'Emma Smith *is a child of* Stephen Smith', for instance. Other examples of relations between people include *is a descendant of* and *lives in the same street as*. An example of a relation between other types of object is *shares a border with*, between countries of the world. For instance, we might say 'France *shares a border with* Germany'.

In mathematics, too, we often work with relations between objects. For example, *is a multiple of* is a relation between the numbers in the set $\mathbb{N}$. Thus we can make statements such as '6 *is a multiple of* 3', which is true, and '5 *is a multiple of* 2', which is false. Another example of a mathematical relation is *is parallel to*, applied to the lines in the plane.

It is sometimes useful to denote a mathematical relation by a symbol, and in this module we usually use the symbol $\sim$. For example, if we use $\sim$ to denote the relation *is a multiple of*, then we write the statement '6 *is a multiple of* 3' as $6 \sim 3$. The symbol $\sim$ is known as *tilde* (pronounced 'tilder'), and in mathematics is usually read as 'twiddles'. So you can read the statement $6 \sim 3$ as '6 twiddles 3'. Alternatively, you can read it as '6 is related to 3'. (In some texts you may see the symbol R rather than $\sim$ used for 'is related to', so $6 \sim 3$ would be written as $6\,R\,3$.)

Some frequently used relations have their own special symbols. For example, the relation *is less than* is usually denoted by the special symbol $<$. Examples of the use of this symbol are the statement $-2 < 1$, which is true, and the statements $1 < -2$ and $3 < 3$, which are both false.

Here is a precise definition of what we mean by a relation.

Definition

We say that $\sim$ is a **relation** on a set X if, whenever $x, y \in X$, the statement $x \sim y$ is either true or false.

If $\sim$ is a relation on a set X and $x \sim y$ is false for a particular pair of elements x and y in X, then we write $x \not\sim y$.

Here are some more examples of relations.

1. *Is equal to* is a relation on the set $\mathbb{R}$. This is because, for any x, y in $\mathbb{R}$, the statement 'x is equal to y' is either definitely true or definitely false. This relation is usually denoted by the special symbol $=$. For instance, the statement $3 = 3$ is true, and the statement $3 = 7$ is false. The relation '$=$' has the unusual property that for any real number x, the only real number y such that $x = y$ is x itself.

2. *Is the derivative of* is a relation on any set of functions. We can define

   $$g \sim f \quad \text{if } g \text{ is the derivative of } f.$$

   For example, let f, g and h be the real functions given by $f(x) = x^3$, $g(x) = 3x^2$ and $h(x) = 2e^x$. Then $g \sim f$ because g is the derivative of f, and $h \sim h$ because h is the derivative of h, but $f \not\sim g$ because f is not the derivative of g.

3. On $\mathbb{C}$, we can define a relation

   $$z_1 \sim z_2 \quad \text{if } |z_1 - z_2| \leq 4;$$

   that is, $z_1 \sim z_2$ if the distance between z_1 and z_2 in the complex plane is less than or equal to 4. For example, $(1 + i) \sim (2 - i)$ because

   $$|(1 + i) - (2 - i)| = |-1 + 2i| = \sqrt{5} \leq 4,$$

   but $(1 + i) \not\sim (3 + 5i)$ because

   $$|(1 + i) - (3 + 5i)| = |-2 - 4i| = \sqrt{20} = 2\sqrt{5} > 4$$

   (see Figure 3).

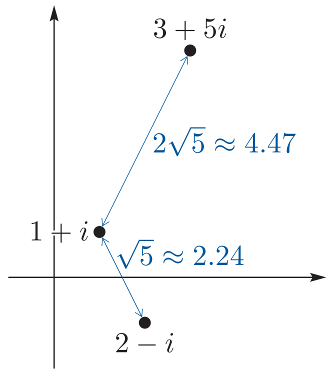


Figure 3 Some distances in the complex plane

Exercise A127

Let $\sim$ be the relation on $\mathbb{N}$ defined by

$$x \sim y \quad \text{if } x \text{ is a divisor of } y.$$

Which of the following statements are true?

(a) $3 \sim 6$ (b) $6 \sim 3$ (c) $6 \sim 18$ (d) $6 \sim 6$

Exercise A128

Let $\sim$ be the relation on $\mathbb{R}$ defined by

$$x \sim y \quad \text{if } x - y \text{ is an integer.}$$

(a) Which of the following statements are true?

  (i) $1.3 \sim 5.3$ (ii) $2.8 \sim 2.1$ (iii) $2.4 \sim -5.4$

(b) (i) Write down a real number y such that $0.8 \sim y$.

  (ii) Write down a real number z such that $0.8 \not\sim z$.

In this section we are mainly interested in relations of a type known as *equivalence relations*. These are relations that have three special properties, as defined below.

Definition

A relation $\sim$ on a set X is an **equivalence relation** if it has the following three properties.

E1 Reflexivity For all x in X,

$$x \sim x.$$

E2 Symmetry For all x, y in X,

$$\text{if } x \sim y, \text{ then } y \sim x.$$

E3 Transitivity For all x, y, z in X,

$$\text{if } x \sim y \text{ and } y \sim z, \text{ then } x \sim z.$$

If a relation has the first, second or third property above, then we say that it is **reflexive**, **symmetric** or **transitive**, respectively.

The three properties reflexivity, symmetry and transitivity are independent in the sense that relations exist with every combination of the three properties.

Note that if a relation $\sim$ is symmetric, then $x \sim y$ and $y \sim x$ mean the same, and we can write either of these interchangeably. For example, the relation $=$ on $\mathbb{R}$ is symmetric, so $x = y$ and $y = x$ mean the same. The relation $<$ on $\mathbb{R}$ is not symmetric, so $x < y$ and $y < x$ mean different things.

To help you understand the three properties, it can be helpful to think through whether they hold for some non-mathematical relations, as in the next worked exercise.

Worked Exercise A72

For each of the following non-mathematical relations on a set of people, state whether the relation is reflexive, symmetric and transitive, briefly justifying your answers, and hence state whether the relation is an equivalence relation.

(a) ‘lives on the same street as’

(b) ‘is a descendant of’

Solution

(a) **E1** The relation 'lives on the same street as' is reflexive, because each person lives on the same street as themselves.

E2 It is also symmetric, because if person A lives on the same street as person B, then it follows that person B lives on the same street as person A.

E3 Finally, it is transitive, because if person A lives on the same street as person B, and person B lives on the same street as person C, then person A lives on the same street as person C.

Hence this relation is an equivalence relation.

(b) **E1** The relation 'is a descendant of' is not reflexive, because a person is not a descendant of themselves.

E2 Nor is it symmetric, because if person A is a descendant of person B, then it does not follow that person B is a descendant of person A.

E3 However, it is transitive, because if person A is a descendant of person B, and person B is a descendant of person C, then it follows that person A is a descendant of person C.

Since this relation is not reflexive (or symmetric), it is not an equivalence relation.

Exercise A129

For each of the following non-mathematical relations on a set of people, state whether the relation is reflexive, symmetric and transitive, briefly justifying your answers, and hence state whether the relation is an equivalence relation.

(a) 'has sat next to'

(b) 'was born in the same year as'

Here are two mathematical examples.

Worked Exercise A73

For each of the following relations on the set $\mathbb{R}$, state whether the relation is reflexive, symmetric and transitive, briefly justifying your answers, and hence state whether the relation is an equivalence relation.

(a) $=$ (b) $<$

Solution

(a) **E1** The relation $=$ is reflexive, since, for all $x \in \mathbb{R}$, $x = x$.

E2 It is also symmetric, since, for all $x, y \in \mathbb{R}$, if $x = y$, then $y = x$.

E3 Finally, it is transitive, since, for all $x, y, z \in \mathbb{R}$, if $x = y$ and $y = z$, then $x = z$.

Hence this relation is an equivalence relation.

(b) **E1** The relation $<$ is not reflexive, since, for example, it is not true that $1 < 1$.

E2 Nor is it symmetric, since, for example, $1 < 2$ but it is not true that $2 < 1$.

E3 However, it is transitive, since, for all $x, y, z \in \mathbb{R}$, if $x < y$ and $y < z$, then $x < z$.

Since this relation is not reflexive (or symmetric), it is not an equivalence relation.

Notice that the statements that you need to prove to show that a relation is reflexive, symmetric or transitive, which are given in the definition in the box shortly before Worked Exercise A72, start with the words 'For all' and are therefore *universal statements*. So to show that a relation $\sim$ on a set X is reflexive, for example, you must show that $x \sim x$ *for all* elements x in X: it is not enough to show that there exists an element x in X such that $x \sim x$. To show that a relation $\sim$ on a set X is *not* reflexive, you just have to show that there is a counterexample – that is, an element x in X such that $x \not\sim x$.

Similarly, to show that a relation $\sim$ on a set X is symmetric, you must prove that $x \sim y \implies y \sim x$ for *every* $x, y \in X$, while to show that it is *not* symmetric, you just have to show that there is a counterexample, that is, a pair $x, y \in X$ for which this property does not hold. Analogous statements hold for the transitive property, involving triples $x, y, z \in X$.

Here is a worked exercise involving two mathematical relations that are more complicated than $=$ and $<$. You met these two relations earlier in this subsection.

Worked Exercise A74

For each relation below, determine whether it has the reflexive, symmetric and transitive properties, and hence state whether it is an equivalence relation.

(a) The relation $\sim$ defined on $\mathbb{C}$ by

$$z_1 \sim z_2 \quad \text{if } |z_1 - z_2| \leq 4.$$

(b) The relation $\sim$ defined on $\mathbb{R}$ by

$$x \sim y \quad \text{if } x - y \text{ is an integer.}$$

Solution

(a) **E1** Let $z \in \mathbb{C}$. Then

$$|z - z| = 0 \leq 4,$$

so $z \sim z$. Thus $\sim$ is reflexive.

E2 Let $z_1, z_2 \in \mathbb{C}$, and suppose that $z_1 \sim z_2$. Then $|z_1 - z_2| \leq 4$, so

$$|z_2 - z_1| = |z_1 - z_2| \leq 4.$$

Hence $z_2 \sim z_1$. Thus $\sim$ is symmetric.

E3 The relation $\sim$ is not transitive, as demonstrated by the example $z_1 = 0$, $z_2 = 3$, $z_3 = 6$ (illustrated in Figure 4):

$$|z_1 - z_2| = |0 - 3| = |-3| = 3 \leq 4, \quad \text{so } z_1 \sim z_2,$$
$$|z_2 - z_3| = |3 - 6| = |-3| = 3 \leq 4, \quad \text{so } z_2 \sim z_3,$$

but

$$|z_1 - z_3| = |0 - 6| = |-6| = 6 > 4, \quad \text{so } z_1 \not\sim z_3.$$

Since $\sim$ is not transitive, it is not an equivalence relation.

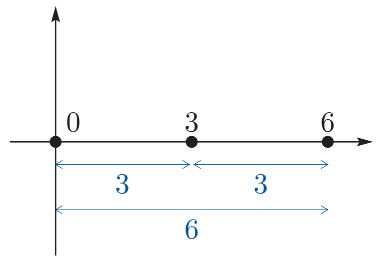


Figure 4 Some distances in the complex plane

(b) **E1** Let $x \in \mathbb{R}$. Then $x - x = 0$, which is an integer. Thus $\sim$ is reflexive.

E2 Let $x, y \in \mathbb{R}$, and suppose that $x \sim y$. Then $x - y$ is an integer, say

$$x - y = k,$$

where $k \in \mathbb{Z}$. It follows that

$$y - x = -(x - y) = -k,$$

which is an integer. Hence $y \sim x$. Thus $\sim$ is symmetric.

E3 Let $x, y, z \in \mathbb{R}$, and suppose that $x \sim y$ and $y \sim z$. Then $x - y$ and $y - z$ are integers, say

$$x - y = k \quad \text{and} \quad y - z = m,$$

where $k, m \in \mathbb{Z}$.

We notice that $(x - y) + (y - z) = x - z$.

We have

$$x - z = x - y + y - z = k + m,$$

which is an integer. Hence $x \sim z$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

Here is a similar exercise for you to try. In part (e), note that in this unit we will take the definition of **parallel** to be 'in the same direction as'. Thus any line is parallel to itself. In fact the word *parallel* may be defined to have either of two possible meanings: the meaning just mentioned, and the one given in Unit A1 in which two lines are *parallel* if they never meet. Both definitions are accepted in mathematics; the only difference between them is that with the definition in Unit A1 a line is not parallel to itself.

Part (f) of the exercise involves the *integer part* of a real number. For any real number x, the **integer part** of x (also called the **floor** of x), denoted by $\lfloor x \rfloor$, is the largest integer that is less than or equal to x. (You will meet this again in your study of functions in Unit A4 *Real functions, graphs and conics*.) For example, $\lfloor 4.3 \rfloor = 4$, $\lfloor -4.3 \rfloor = -5$ and $\lfloor 4 \rfloor = 4$. So, for any real number x, the integer part $\lfloor x \rfloor$ of x is obtained by rounding down to the nearest integer; the rounding is always *down*, no matter whether x is positive or negative.

Exercise A130

For each relation below, determine whether it has the reflexive, symmetric and transitive properties, and hence state whether it is an equivalence relation.

(a) The relation $\sim$ defined on $\mathbb{Z}$ by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(b) The relation $\sim$ defined on $\mathbb{Z}$ by

$$m \sim n \quad \text{if } m - n \text{ is odd.}$$

(c) The relation $\sim$ defined on $\mathbb{Z}$ by

$$m \sim n \quad \text{if } m^2 + n^2 \text{ is even.}$$

(d) The relation $\sim$ defined on $\mathbb{C}$ by

$$z_1 \sim z_2 \quad \text{if } |z_1| = |z_2|.$$

(e) The relation $\sim$ defined on the set of all lines in the plane by

$$l_1 \sim l_2 \quad \text{if the lines } l_1 \text{ and } l_2 \text{ are parallel.}$$

(f) The relation $\sim$ defined on $\mathbb{R}$ by

$$x \sim y \quad \text{if } \lfloor x - y \rfloor = 0.$$

You have already met an important family of equivalence relations in Unit A2. Let n be any integer greater than 1, and consider the relation *is congruent modulo n to* on the set $\mathbb{Z}$. As you have seen, this relation is usually denoted by the special symbol $\equiv$, and we usually also include '(mod n)' to make it clear which value of n we are working with. For example, with $n = 7$, the statement

$$1 \equiv 8 \pmod{7}$$

is true, and the statement

$$1 \equiv 12 \pmod{7}$$

is false.

You saw in Unit A2 that the reflexive, symmetric and transitive properties hold for congruence modulo n; these properties are the first three properties in Theorem A10 in that unit. So we have the following theorem.

Theorem A15

For any integer $n > 1$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Very roughly, you can think of any equivalence relation as a relation that defines some kind of 'equivalence' on the objects in the set on which the relation is defined.

For example, with the equivalence relation *was born in the same year as* on a set of people, two people are 'equivalent' if they were born in the same year. Imagine that you are selecting people to take part in a survey, and the only selection criterion is that you need to select ten people born in each year from 1950 to 1999. Then, as far as selecting people for the survey is concerned, you would consider two people to be 'equivalent' if they were born in the same year. For instance, if Ashok and Becky were both born in 1992, then it doesn't matter which of them you select: they are equivalent.

Here are two mathematical examples. First, with the equivalence relation *is equal to* on the set $\mathbb{R}$, two real numbers are 'equivalent' if they are equal. This is a very strict type of equivalence, where two objects are 'equivalent' only if they are exactly the same (though they might be written differently, such as $\frac{1}{2}$, $\frac{3}{6}$ and 0.5).

Second, with the equivalence relation in Exercise A130(e), two lines in the plane are 'equivalent' if they are parallel. This equivalence between lines might be useful if we were interested only in the directions of lines and not in their positions in the plane.

With the equivalence relation congruence modulo n, two integers are 'equivalent' if they have the same remainder on division by n. We use this type of equivalence when we carry out modular arithmetic.

Finally in this subsection, here is an interesting 'spot the error' exercise. It involves an incorrect proof that appears to show that if a relation is both symmetric and transitive, then it is also reflexive. If this were true, then we could define an equivalence relation to be a relation that is symmetric and transitive – we could omit the condition that it must also be reflexive. However, it is not true, as you are asked to show in the exercise. The error in the proof is very subtle. It highlights just how careful we need to be in mathematical arguments.

Exercise A131

Consider the following incorrect claim and incorrect proof.

Claim (incorrect)

Let $\sim$ be a relation on a set X. If $\sim$ is symmetric and transitive, then $\sim$ is also reflexive.

Proof (incorrect) Suppose that $\sim$ is symmetric and transitive. We will show that $\sim$ is then also reflexive. Let $x \in X$. We have to show that $x \sim x$. Let y be an element of X such that $x \sim y$. Then, since $\sim$ is symmetric, we have $y \sim x$. Since $x \sim y$ and $y \sim x$, and $\sim$ is transitive, we have $x \sim x$, as required. Thus $\sim$ is reflexive. ■

(a) Show that the claim is incorrect by demonstrating that the relation $\sim$ defined on $\mathbb{R}$ by

$$x \sim y \quad \text{if } xy > 0$$

is a counterexample. That is, you have to show that this relation $\sim$ is symmetric and transitive, but not reflexive.

(b) Try to spot the error in the given proof. (Do not worry if you cannot spot it, as it is subtle, but be impressed with yourself if you can! Make sure to look at the answer.)

4.2 Equivalence classes

We now look at the idea of an *equivalence class*. This idea is associated only with equivalence relations, not with relations in general.

Definition

Let $\sim$ be an equivalence relation on a set X, and let $x \in X$. Then the **equivalence class** of x, denoted by $[\![x]\!]$, is the set

$$[\![x]\!] = \{y \in X : x \sim y\}.$$

In other words, $[\![x]\!]$ is the set of all the elements in X that are related to x by the equivalence relation; that is, it is the set of all the elements in X that are equivalent to x, where the equivalence is given by the equivalence relation. Notice that $[\![x]\!]$ includes the element x itself, because for an equivalence relation we have $x \sim x$.

For example, consider the equivalence relation *was born in the same year as* on a set of people. The equivalence class of a particular person is the set of people who were born in the same year as that person, including the person themself.

As a mathematical example, consider the equivalence relation on the set of lines in the plane defined by

$$l_1 \sim l_2 \quad \text{if the lines } l_1 \text{ and } l_2 \text{ are parallel.}$$

You saw that this relation is an equivalence relation in Exercise A130(e). Consider any particular line l in the plane. Then the equivalence class $[\![l]\!]$ of l is the set of all the lines in the plane that are parallel to l, including l itself.

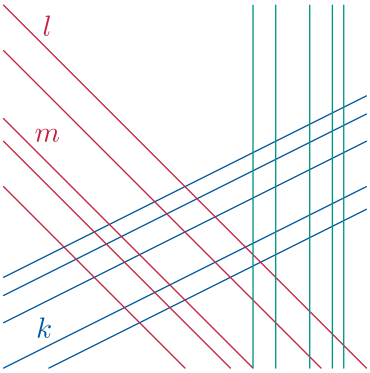


Figure 5 Lines in the plane

Let us think about this example a little more. Consider a particular line l, as illustrated in Figure 5. Notice if you choose any line, say m, that lies in the equivalence class $[\![l]\!]$ of l, then $[\![m]\!]$ and $[\![l]\!]$ are in fact the *same set*. On the other hand, if you choose a line, say k, that is *not* in the equivalence class $[\![l]\!]$ of the original line l, then not only are the two sets $[\![k]\!]$ and $[\![l]\!]$ different sets, but in fact they are *disjoint* sets. (Remember that two sets are said to be **disjoint** if they have no elements in common.)

In fact, you can see that essentially what has happened here is that the set of all the lines in the plane has been split into a collection of subsets, with each subset consisting of all the lines in a particular direction.

So the equivalence classes of this particular equivalence relation split the set on which the relation is defined into a collection of subsets, such that each pair of these subsets is disjoint. Such a collection of subsets is known as a *partition* of the set, as defined below and illustrated in Figure 6.

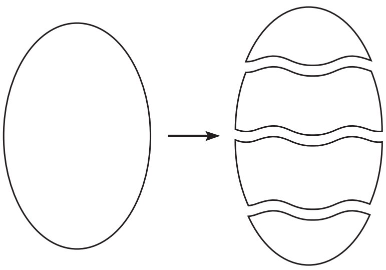


Figure 6 Partitioning a set

Definitions

A collection of non-empty subsets of a set is a **partition** of the set if every pair of subsets in the collection is disjoint and the union of all the subsets in the collection is the whole set.

We say that such a collection of subsets **partitions** the set.

In other words, a collection of non-empty subsets of a set is a partition of the set if *every* element of the set belongs to *exactly one* of the subsets in the collection.

In fact, for *every* equivalence relation, its equivalence classes form a partition of the set on which the relation is defined, as stated and proved below.

Theorem A16

The equivalence classes of an equivalence relation on a set X form a partition of the set X.

Proof First, since every element x of X belongs to an equivalence class, namely its own equivalence class $[\![x]\!]$, the union of the equivalence classes of $\sim$ is the whole set X.

To prove that the equivalence classes of $\sim$ partition the set X, the other property that we have to show is that if x and y are any elements of X, then their equivalence classes $[\![x]\!]$ and $[\![y]\!]$ are either the *same* subset of X, or *disjoint* subsets of X. We can prove this as follows.

Let x and y be elements of X, and suppose that $[\![x]\!]$ and $[\![y]\!]$ are *not* disjoint, that is, they have at least one element in common, say z. We will show that $[\![x]\!]$ and $[\![y]\!]$ must then be the same set, that is, $[\![x]\!] = [\![y]\!]$.

To do this, we use the strategy for proving that two sets are equal given in Unit A1: we show that each set is a subset of the other.

First we show that $\llbracket x \rrbracket \subseteq \llbracket y \rrbracket$. Suppose that $a \in \llbracket x \rrbracket$; we have to show that $a \in \llbracket y \rrbracket$. Since both a and z are in $\llbracket x \rrbracket$, we know that $x \sim a$ and $x \sim z$. Hence (since the relation $\sim$ is symmetric and transitive) we have $a \sim z$. But we also know that $y \sim z$, because $z \in \llbracket y \rrbracket$, so (again since $\sim$ is symmetric and transitive) it follows that $y \sim a$. Hence $a \in \llbracket y \rrbracket$, as claimed.

We can show in the same way that $\llbracket y \rrbracket \subseteq \llbracket x \rrbracket$ (we interchange the roles of x and y in the proof that $\llbracket x \rrbracket \subseteq \llbracket y \rrbracket$).

Hence $\llbracket x \rrbracket = \llbracket y \rrbracket$. This completes the proof. ∎

The proposition below was proved as part of the proof of Theorem A16 above, and you saw it illustrated for a particular equivalence relation (the one involving lines in the plane) near the start of this subsection. It is an important fact to keep in mind when you are working with equivalence classes.

Proposition A17

The equivalence classes of an equivalence relation on a set X have the following property: if x and y are elements of X, then their equivalence classes $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$ are either equal sets or disjoint sets.

If you think about an equivalence relation as defining a type of 'equivalence', then Theorem A16 seems true intuitively. Each equivalence class is a subset of elements that are all 'equivalent' to each other. Each element lies in such a class, and each element is not equivalent to any element outside its own class.

As an example of Theorem A16, consider the equivalence relation *was born in the same year as* on a set of people. The equivalence class of each person is the set of people born in the same year as that person. So the whole set of people is partitioned into a set of classes: the class of people born in 1966, the class of people born in 1992, the class of people born in 2001, and so on. Each person belongs to one of these classes, and each pair of the classes is disjoint.

As a mathematical example of Theorem A16, consider the equivalence relation *is equal to* on $\mathbb{R}$. Consider any number $x \in \mathbb{R}$. Since $x = y$ only if y is the same number as x, the equivalence class of the real number x contains only the number x itself. So each element lies in a single-element equivalence class, as illustrated in Figure 7. For example, $\llbracket 0 \rrbracket = \{0\}$, $\llbracket 1 \rrbracket = \{1\}$, and so on.

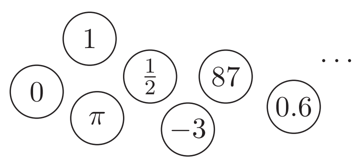


Figure 7 Some equivalence classes of 'is equal to'

As another mathematical example of Theorem A16, consider the equivalence relation *congruence modulo 5* defined on $\mathbb{Z}$. The equivalence class of 0 is the subset of $\mathbb{Z}$ containing all the integers that are congruent to 0 modulo 5. Similarly, the equivalence class of 1 is the subset of $\mathbb{Z}$ containing all the integers that are congruent to 1 modulo 5, and so on. That is,

$$\begin{aligned}
\llbracket 0 \rrbracket &= \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\},\\
\llbracket 1 \rrbracket &= \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\},\\
\llbracket 2 \rrbracket &= \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\},\\
\llbracket 3 \rrbracket &= \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\},\\
\llbracket 4 \rrbracket &= \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}$$

There are only five *distinct* equivalence classes since, for example, $\llbracket 5 \rrbracket$ is the same set as $\llbracket 0 \rrbracket$, and $\llbracket 6 \rrbracket$ is the same set as $\llbracket 1 \rrbracket$, and so on. The collection of five equivalence classes partitions the set $\mathbb{Z}$, as illustrated in Figure 8: every number in $\mathbb{Z}$ belongs to one of the five classes, and the five classes are all disjoint from each other.

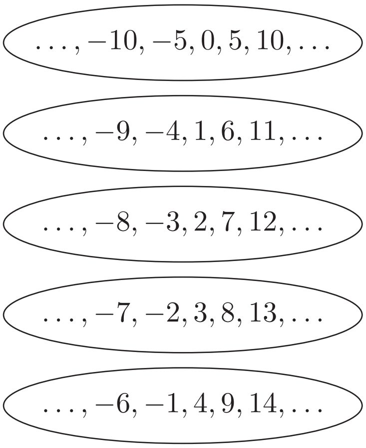


Figure 8 The five equivalence classes of congruence modulo 5

In general, congruence modulo n partitions the set $\mathbb{Z}$ into n distinct equivalence classes.

Notice that an equivalence class of an equivalence relation may be a finite set or an infinite set, and that an equivalence relation may have finitely many equivalence classes or infinitely many equivalence classes.

The next worked exercise involves finding a particular equivalence class of another equivalence relation.

Worked Exercise A75

Find the equivalence class $\llbracket 3.7 \rrbracket$ of the equivalence relation defined on $\mathbb{R}$ by

$$x \sim y \quad \text{if } x - y \text{ is an integer.}$$

(You saw that this relation is an equivalence relation in Worked Exercise A74(b).)

Solution

Apply the definition of an equivalence class, then try to express the resulting set in as simple a way as possible without using the symbol $\sim$, to make it clear what the elements of the set are.

We have

$$\begin{aligned}
\llbracket 3.7 \rrbracket &= \{y \in \mathbb{R} : 3.7 \sim y\}\\
&= \{y \in \mathbb{R} : 3.7 - y \text{ is an integer}\}\\
&= \{y \in \mathbb{R} : 3.7 - y = k \text{ for some } k \in \mathbb{Z}\}\\
&= \{y \in \mathbb{R} : y = 3.7 - k \text{ for some } k \in \mathbb{Z}\}
\end{aligned}$$

The set of real numbers y such that $y = 3.7 - k$ for some integer k is the same as the set of real numbers y such that $y = 3.7 + k$ for some integer k. And we can write $3.7 + k$ as $k + 3.7$.

$$= \{y \in \mathbb{R} : y = k + 3.7 \text{ for some } k \in \mathbb{Z}\}$$

The set of real numbers y such that $y = k + 3.7$ for some integer k is, more simply, the set of numbers of the form $k + 3.7$ for some integer k.

$$= \{k + 3.7 : k \in \mathbb{Z}\}$$

Saying that an integer is of the form 'some integer plus 3.7' is the same as saying that it is of the form 'some integer plus 0.7'. The latter is slightly simpler.

$$= \{k + 0.7 : k \in \mathbb{Z}\}.$$

This set can also be written (less concisely) as

$$[\![3.7]\!] = \{\ldots,\ -2.3,\ -1.3,\ -0.3,\ 0.7,\ 1.7,\ 2.7,\ 3.7,\ \ldots\}.$$

Exercise A132

Find the equivalence class $[\![1]\!]$ of the equivalence relation $\sim$ defined on $\mathbb{Z}$ by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(You saw that this relation is an equivalence relation in Exercise A130(a).)

If we want to find *all* the equivalence classes of an equivalence relation, then it often helps to start by finding a particular equivalence class, or a few particular equivalence classes, as demonstrated in the next worked exercise. This can help us to see what happens in general.

Worked Exercise A76

Let $\sim$ be the equivalence relation defined on $\mathbb{C}$ by

$$z_1 \sim z_2 \quad \text{if } |z_1| = |z_2|.$$

(You saw that this relation is an equivalence relation in Exercise A130(d).)

(a) Find the equivalence classes $[\![0]\!]$ and $[\![i]\!]$.

(b) Describe all the equivalence classes of $\sim$.

Solution

(a) We have

$$\begin{aligned}[\![0]\!] &= \{z \in \mathbb{C} : 0 \sim z\} \\ &= \{z \in \mathbb{C} : |0| = |z|\} \\ &= \{z \in \mathbb{C} : |z| = 0\} \\ &= \{0\}.\end{aligned}$$

So $[\![0]\!]$ is the set containing the complex number 0 alone.

Similarly,

$$\begin{aligned}[\![i]\!] &= \{z \in \mathbb{C} : i \sim z\} \\ &= \{z \in \mathbb{C} : |i| = |z|\} \\ &= \{z \in \mathbb{C} : |z| = 1\}.\end{aligned}$$

So $[\![i]\!]$ is the set of all complex numbers of modulus 1.

(b) In general, for any complex number z_0, say, we have

$$\begin{aligned}[\![z_0]\!] &= \{z \in \mathbb{C} : z_0 \sim z\} \\ &= \{z \in \mathbb{C} : |z_0| = |z|\} \\ &= \{z \in \mathbb{C} : |z| = |z_0|\}.\end{aligned}$$

So $[\![z_0]\!]$ is the set of all complex numbers with the same modulus as z_0.

If $|z_0| = r$, say, then

$$[\![z_0]\!] = \{z \in \mathbb{C} \colon |z| = r\}.$$

This set forms the circle with centre the origin and radius r in the complex plane.

Hence the equivalence classes of $\sim$ are the circles in the complex plane with centre the origin. (The origin is an equivalence class containing just the complex number 0; it can be thought of as a circle of radius 0.)

Some of the equivalence classes of the equivalence relation in Worked Exercise A76 are illustrated in Figure 9. They are the circles with centre the origin, together with the origin itself. Notice that, as expected, the equivalence classes partition the set on which the equivalence relation is defined.

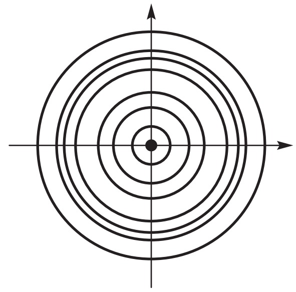


Figure 9 Some equivalence classes of the equivalence relation in Worked Exercise A76

Exercise A133

Determine all the equivalence classes of the equivalence relation $\sim$ defined on $\mathbb{Z}$ by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(You saw that this relation is an equivalence relation in Exercise A130(a), and you were asked to find the equivalence class $[\![1]\!]$ of this relation in Exercise A132.)

Exercise A134

Let $\sim$ be the relation defined on $\mathbb{R}$ by

$$x \sim y \quad \text{if } \lfloor x \rfloor = \lfloor y \rfloor.$$

(Remember that $\lfloor x \rfloor$ denotes the integer part of x: the largest integer that is less than or equal to x; for example $\lfloor 4.72 \rfloor = 4$.)

(a) Show that $\sim$ is an equivalence relation.

(b) Determine the equivalence classes $[\![1]\!]$ and $[\![-4]\!]$.

(c) Describe all the equivalence classes of $\sim$.

As a further exercise on equivalence classes, you are asked next to prove the converse of Theorem A16, namely that every partition of a set X gives rise to an equivalence relation on X whose equivalence classes are the subsets that make up the partition.

Exercise A135

Let X be a set, and suppose we are given a collection of non-empty subsets of X that forms a partition of X. Let $\sim$ be the relation defined on X by

$$x \sim y \quad \text{if } x \text{ and } y \text{ belong to the same subset in the partition.}$$

Show that $\sim$ is an equivalence relation on X.

Representatives of equivalence classes

You have seen that if $\sim$ is an equivalence relation on a set X, and x and y are two elements of X such that $x \sim y$, then $[\![x]\!] = [\![y]\!]$. Thus, in general, there is more than one way to denote each equivalence class using the notation $[\![\ ]\!]$: a class can be denoted by $[\![x]\!]$ where x is any one of its elements. For example, consider again the equivalence classes of the equivalence relation congruence modulo 5:

$$\begin{aligned}
[\![0]\!] &= \{\dots, -10, -5, 0, 5, 10, 15, \dots\},\\
[\![1]\!] &= \{\dots, -9, -4, 1, 6, 11, 16, \dots\},\\
[\![2]\!] &= \{\dots, -8, -3, 2, 7, 12, 17, \dots\},\\
[\![3]\!] &= \{\dots, -7, -2, 3, 8, 13, 18, \dots\},\\
[\![4]\!] &= \{\dots, -6, -1, 4, 9, 14, 19, \dots\}.
\end{aligned}$$

We can denote the first equivalence class here by $[\![0]\!]$, or by $[\![5]\!]$, or by $[\![-5]\!]$, and so on. Similarly, we can denote the second equivalence class by $[\![1]\!]$, or by $[\![6]\!]$, or by $[\![-4]\!]$, and so on; and similarly for the other equivalence classes.

When we are working with an equivalence relation, it is sometimes useful to choose a particular element x in each equivalence class and normally denote the class by $[\![x]\!]$. The element x that we choose is called a **representative** of the class.

For example, for the equivalence relation congruence modulo 5, whose equivalence classes are listed above, the most convenient representatives for the five classes are 0, 1, 2, 3 and 4.

In general, if $\sim$ is an equivalence relation on a set X, then a set of elements of X that contains exactly one element from each equivalence class of $\sim$ is called a **set of representatives** for the equivalence relation $\sim$. For example, $\{0, 1, 2, 3, 4\}$ is a set of representatives for congruence modulo 5.

More generally, for any integer $n \geq 2$, the equivalence relation congruence modulo n has n equivalence classes, and the most convenient set of representatives for them is $\{0, 1, 2, \dots, n-1\}$, as set out below.

$$\begin{aligned}
[\![0]\!] &= \{\dots, -2n, -n, 0, n, 2n, \dots\},\\
[\![1]\!] &= \{\dots, 1-2n, 1-n, 1, 1+n, 1+2n, \dots\},\\
&\ \ \vdots\\
[\![n-1]\!] &= \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}.
\end{aligned}$$

In other words, the most convenient set of representatives for the equivalence relation congruence modulo n is the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, which you worked with in Subsection 3.3 of Unit A2. The definitions of the modular operations $+_n$ and $\times_n$ can be rephrased in terms of the equivalence classes of the equivalence relation congruence modulo n, as follows.

For all $a, b \in \mathbb{Z}_n$,

$a +_n b$ is the integer in $\mathbb{Z}_n$ that lies in the class $[\![a + b]\!]$,

$a \times_n b$ is the integer in $\mathbb{Z}_n$ that lies in the class $[\![a \times b]\!]$.

For example, in $\mathbb{Z}_5$,

$$3 +_5 4 = 2,$$

because $3 + 4 = 7$ and the equivalence class $[\![7]\!]$ of congruence modulo 5 contains the element 2 of $\mathbb{Z}_5$.

Exercise A136

Use the definitions of $+_n$ and $\times_n$ above to calculate $4 +_5 4$ and $3 \times_5 4$, writing out the details of your working.

As another example of using representatives for equivalence classes, consider again the equivalence relation $\sim$ defined on $\mathbb{C}$ by

$$z_1 \sim z_2 \quad \text{if } |z_1| = |z_2|.$$

The equivalence classes of this equivalence relation were found in Worked Exercise A76 to be all the sets of the form

$$\{z \in \mathbb{C} \colon |z| = r\},$$

where $r \in \mathbb{R}$. That is, they are the circles in the complex plane with centre the origin, including the origin itself as a ‘circle of radius 0’.

Consider the particular equivalence class

$$\{z \in \mathbb{C} : |z| = 4\},$$

that is, the circle of radius 4, which is shown in Figure 10(a). This class contains the complex numbers 4, $-4i$ and $-2\sqrt{2}(1+i)$, for example, since all these complex numbers have modulus 4. So we could denote this equivalence class by any of $[\![4]\!]$, $[\![-4i]\!]$ or $[\![-2\sqrt{2}(1+i)]\!]$, for example. We might decide that it is convenient to choose the representative 4, and denote the class by $[\![4]\!]$. In general, the equivalence class

$$\{z \in \mathbb{C} : |z| = r\},$$

of this equivalence relation contains the element r and so can be denoted by $[\![r]\!]$. Some examples of this choice of representatives are shown in Figure 10(b).

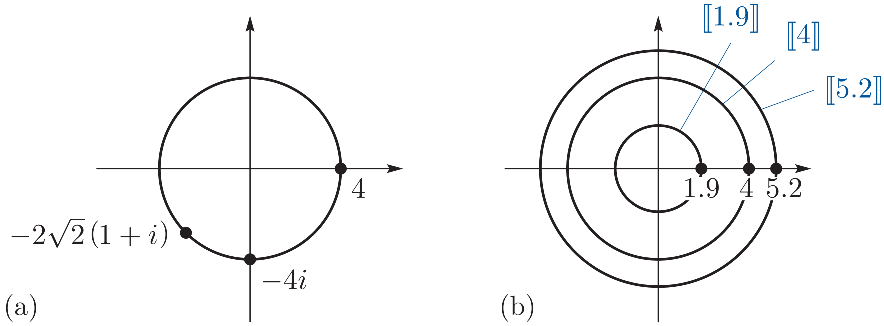


Figure 10 For the equivalence relation given by $z_1 \sim z_2$ if $|z_1| = |z_2|$: (a) a particular equivalence class (b) some equivalence classes with representatives

A set of complex numbers that contains exactly one element from each equivalence class of the equivalence relation $\sim$ is the set $[0, \infty)$, the set of all non-negative real numbers. So $[0, \infty)$ is a set of representatives for $\sim$.

Exercise A137

Describe a set of representatives for each of the following equivalence relations.

(a) The relation $\sim$ defined on $\mathbb{Z}$ by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(You saw that $\sim$ is an equivalence relation in Exercise A130(a), and you were asked to find its equivalence classes in Exercise A133.)

(b) The relation $\sim$ defined on $\mathbb{R}$ by

$$x \sim y \quad \text{if } \lfloor x \rfloor = \lfloor y \rfloor.$$

(You were asked to show that $\sim$ is an equivalence relation, and find its equivalence classes, in Exercise A134.)

Congruence modulo 2π

To end this subsection we look at an equivalence relation that is similar to congruence modulo n on $\mathbb{Z}$, but which is defined on $\mathbb{R}$ rather than $\mathbb{Z}$, and in which the modulus is 2π, rather than an integer n. You will see that this equivalence relation enables us to express concisely some results about complex numbers.

This relation is the relation $\sim$ defined on $\mathbb{R}$ by

$$x \sim y \quad \text{if } x - y = 2\pi k \text{ for some integer } k.$$

We begin by showing that this relation actually is an equivalence relation.

E1 Let $x \in \mathbb{R}$. Then $x - x = 0 = 2\pi \times 0$, so $x \sim x$. Thus $\sim$ is reflexive.

E2 Let $x, y \in \mathbb{R}$ and suppose that $x \sim y$. Then

$$x - y = 2\pi k$$

for some integer k. Hence

$$y - x = 2\pi(-k).$$

Since $-k$ is an integer, this shows that $y \sim x$. Thus $\sim$ is symmetric.

E3 Let $x, y, z \in \mathbb{Z}$ and suppose that $x \sim y$ and $y \sim z$. Then

$$x - y = 2\pi j \quad \text{and} \quad y - z = 2\pi k$$

for some integers j and k. Hence

$$x - z = x - y + y - z = 2\pi(j + k).$$

Since $j + k$ is an integer, this shows that $x \sim z$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

The equivalence relation $\sim$ above is known as **congruence modulo 2π**. For this equivalence relation, we can use notation similar to the notation that we use for congruence modulo n. That is, rather than writing

$$x \sim y,$$

we can write

$$x \equiv y \pmod{2\pi}.$$

For example,

$$\frac{9\pi}{2} \equiv \frac{\pi}{2} \pmod{2\pi},$$

because

$$\frac{9\pi}{2} - \frac{\pi}{2} = 2 \times 2\pi.$$

You have seen that congruence modulo n on $\mathbb{Z}$ corresponds to modular arithmetic on the set $\mathbb{Z}_n$, which is a set of representatives of the equivalence classes of congruence modulo n. In a similar way, congruence modulo 2π on $\mathbb{R}$ corresponds to modular arithmetic on a set of representatives of the equivalence classes of congruence modulo 2π.
The equivalence classes of $\sim$ are the sets of the form

$$[\![x]\!] = \{x + 2n\pi : n \in \mathbb{Z}\},$$

where $x \in \mathbb{R}$. For example, one equivalence class is

$$[\![0]\!] = \{\ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \ldots\},$$

and another is

$$\left[\!\!\left[\frac{\pi}{2}\right]\!\!\right] = \left\{\ldots, -\frac{7\pi}{2}, -\frac{3\pi}{2}, \frac{\pi}{2}, \frac{5\pi}{2}, \frac{9\pi}{2}, \ldots\right\}.$$

A suitable set of representatives for the equivalence classes is the interval $(-\pi, \pi]$, since every equivalence class has exactly one representative in this interval. Other intervals can be used, for example $[0, 2\pi)$, but $(-\pi, \pi]$ is useful as it corresponds to our definition of the principal argument of a complex number.

We define modular operations $+_{2\pi}$ and $\times_{2\pi}$ on the interval $(-\pi, \pi]$ as follows. For all $x, y \in (-\pi, \pi]$,

$x +_{2\pi} y$ is the real number in $(-\pi, \pi]$ that lies in the class $[\![x + y]\!]$,

$x \times_{2\pi} y$ is the real number in $(-\pi, \pi]$ that lies in the class $[\![xy]\!]$.

For example,

$$\pi +_{2\pi} \frac{\pi}{2} = -\frac{\pi}{2},$$

since $\pi + \dfrac{\pi}{2} = \dfrac{3\pi}{2}$ and $\left[\!\!\left[\dfrac{3\pi}{2}\right]\!\!\right]$ contains the element $-\dfrac{\pi}{2}$ of $(-\pi, \pi]$. This type of modular arithmetic is effectively what we do when we find the *principal* argument of a complex number arising from some calculation.

Recall that the principal argument of a complex number z is denoted by $\operatorname{Arg} z$. Arithmetic modulo 2π on the interval $(-\pi, \pi]$ gives us a concise way to express some results about complex numbers that involve principal arguments. For example, you saw in Unit A2 that, if z_1 and z_2 are any two complex numbers, then $\operatorname{Arg} z_1 + \operatorname{Arg} z_2$ is an argument of $z_1 z_2$, but is not necessarily the principal argument. The principal argument is $\operatorname{Arg} z_1 +_{2\pi} \operatorname{Arg} z_2$, so we can now state that

$$\operatorname{Arg}(z_1 z_2) = \operatorname{Arg} z_1 +_{2\pi} \operatorname{Arg} z_2.$$

You have now seen what congruence modulo 2π means. For any integer $r \in \mathbb{R}$, we can define congruence modulo r on $\mathbb{R}$ in a similar way to the way that congruence modulo 2π is defined, and it can be checked that this relation is an equivalence relation in a similar way to the argument above. In fact, the equivalence relation in Worked Exercise A74(b) is congruence modulo 1 on $\mathbb{R}$. However, congruence modulo 2π is particularly useful, for the reasons you saw above.

Summary

In this unit you have been working with the bricks and mortar from which mathematics is built – the statements that express mathematical ideas and the proofs that establish which statements are true.

You have met different types of mathematical statements and seen how they can be combined and negated to make new statements. You have encountered several different methods of proof – some direct, such as the Principle of Mathematical Induction, and others indirect, such as proof by contradiction and proof by contraposition. You have also practised writing your own proofs and learned how to critically analyse mathematical arguments.

Skills such as these are not acquired easily, so do not be discouraged if you found some parts of this unit rather hard. There will be many more opportunities to read and write proofs as you work through the remaining units in this module, so your skills will develop as you continue your studies.

Finally, you have been introduced to the important topic of an equivalence relation on a set – a precise way of defining which elements of a set we regard as equivalent or 'the same'. You will make extensive use of equivalence relations in the group theory units of this module.

Learning outcomes

After working through this unit, you should be able to:

- understand what is asserted by various types of mathematical statements, in particular *implications* and *equivalences*
- negate a mathematical statement, including *universal* and *existential* statements
- produce simple proofs of various types, including *direct* proofs, proofs by *induction*, by *contradiction* and by *contraposition*
- disprove a universal statement by providing a *counterexample*
- read and understand the logical structure of more complex proofs
- critically analyse a mathematical argument to identify, explain and rectify mathematical errors
- explain the meanings of a *relation* defined on a set, an *equivalence relation* and a *partition* of a set
- determine whether a relation defined on a set is an equivalence relation by checking the *reflexive*, *symmetric* and *transitive properties*
- understand that an equivalence relation partitions a set into *equivalence classes*, and determine the equivalence classes for an equivalence relation.

Solutions to exercises

Solution to Exercise A101

(a) This is a mathematical statement. Whether the statement is true or false depends on the value of the variable n, so the statement is a variable proposition.

(b) This assertion is not a mathematical statement, as the property of 'being small' has not been defined mathematically, and so it is not precise enough.

(c) Since $\{1, 2, 3, 4\}$ is not an integer, it cannot be even or odd. Therefore this assertion is neither true nor false, and so it is not a mathematical statement.

(d) This is a mathematical statement (a false one). It contains no variable, and so is not a variable proposition.

Solution to Exercise A102

(a) The negation can be expressed as

$x = \frac{3}{5}$ is not a solution of the equation $3x + 5 = 0$.

(b) The negation can be expressed as

The equation $n^2 + n - 2 = 0$ does not have exactly two solutions

or, more precisely, as

The equation $n^2 + n - 2 = 0$ has either no solution, exactly one solution or more than two solutions.

Solution to Exercise A103

(a) The negation is 'it is not the case that both x and y are integers'; that is, 'at least one of x or y is not an integer'. Some equivalent formulations of this negation are

either x or y is not an integer,

or

$$x \notin \mathbb{Z} \text{ or } y \notin \mathbb{Z}.$$

(b) The statement is equivalent to the conjunction 'm is even and n is odd'. The negation can be expressed as

m is odd or n is even.

(c) The statement is equivalent to the disjunction 'm is odd or n is odd'. The negation can be expressed as

the integers m and n are both even.

(d) The negation can be expressed as

$$A \neq \varnothing \text{ and } B \neq \varnothing.$$

Solution to Exercise A104

(a) The statement can be rewritten as

if $x^2 - 2x + 1 = 0$, then $(x-1)^2 = 0$.

This is true.

(b) The statement can be rewritten as

if n is odd, then n^3 is odd.

This is true.

(c) The statement can be rewritten as

if a given integer is divisible by 3, then it is also divisible by 6.

This is false.

(d) The statement can be rewritten as

if $x > 2$, then $x > 4$.

This is false.

(e) The statement can be rewritten as

if $x \leq 0$, then $x^3 \leq 0$.

This is true.

Solution to Exercise A105

(a) The negation is

m and n are odd, and $m + n$ is not odd,

that is,

m and n are odd, and $m + n$ is even.

(b) The negation of '$A \cup B = \varnothing$ or $B - A = \varnothing$' is

$$A \cup B \neq \varnothing \text{ and } B - A \neq \varnothing .$$

Thus the negation of the implication is

$$A = \varnothing, \text{ and } A \cup B \neq \varnothing \text{ and } B - A \neq \varnothing .$$

Solution to Exercise A106

(a) The converse is

if $m + n$ is even, then m and n are both odd.

The given implication is true, and its converse is false.

(b) The converse is

if $m + n$ is odd, then one of the pair m, n is even and the other is odd.

The given implication and its converse are both true.

Solution to Exercise A107

(a) The converse is

if at least one of m or n is even, then mn is even.

The contrapositive is

if both m and n are odd, then mn is odd.

The converse is true, and so is the contrapositive. (Since the contrapositive is true, the original statement is also true).

(b) The converse is

if q divides m or q divides n, then q divides the product mn.

The contrapositive is

if q divides neither m nor n, then q does not divide the product mn.

The converse is true, but the contrapositive (and hence the original statement) is false.

Solution to Exercise A108

(a) The two implications are 'if the product mn is odd, then both m and n are odd', and 'if both m and n are odd, then the product mn is odd'. Both implications are true, so the equivalence is true.

(b) The two implications are 'if the product mn is even, then both m and n are even', and 'if both m and n are even, then the product mn is even'. The first implication is false, and the second is true. As at least one implication is false, the equivalence is false.

Solution to Exercise A109

(a) The negation is

it is not the case that there is a real number x such that $\cos x = x$;

that is,

there is no real number x such that $\cos x = x$.

Another way of expressing this negation is

for all real numbers x, $\cos x \neq x$.

(b) The negation can be expressed as

there is no integer that is divisible by 3 but not by 6,

or, alternatively,

every integer that is divisible by 3 is also divisible by 6.

(c) The negation can be expressed as

there is a real number x that does not satisfy the inequality $x^2 \geq 0$,

or, alternatively,

there is a real number x such that $x^2 < 0$.

Solution to Exercise A110

(a) Suppose that n is an even integer. Then $n = 2k$, where k is an integer, so

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Since $2k^2$ is an integer, this proves that n^2 is even, as required.

(b) Let m and n be multiples of k. Then $m = ka$ and $n = kb$, where a and b are integers. Hence

$$m + n = ka + kb = k(a + b).$$

Since $a + b$ is an integer, we deduce that $m + n$ is a multiple of k, as required.

(c) Suppose that one of the pair m, n is even and the other is odd. Then one of them is equal to $2k$ and the other to $2l+1$, for some integers k and l. Then

$$m+n = 2k + (2l+1) = 2(k+l)+1.$$

Since $k+l$ is an integer, this shows that $m+n$ is odd.

(d) Let n be a positive integer. We note that

$$n^2 + n = n(n+1).$$

Either n or $n+1$ must be even, so their product n^2+n is even, as required.

(Alternatively, the implication can be proved by considering two separate cases: the case where n is even, and the case where n is odd. However, the proof above is shorter and simpler.)

Solution to Exercise A111

The problem lies in the step

$$x+1 \leq 0 \implies (x+1)^2 \leq 0\,.$$

This implication is false: take, for example, $x=-2$. The writer of the deduction seems to have used an incorrect assumption that an inequality is preserved by squaring its two sides, that is, that for real numbers a and b

$$a \leq b \implies a^2 \leq b^2\,.$$

(This implication only holds under the additional assumption that $a \geq 0$.)

Solution to Exercise A112

The problem with this argument is that it starts by assuming the statement to be proved ($|z_1| = |z_2|$) and uses it to deduce a second statement that is known to be true ($5=5$). Deducing a true statement Q from a statement P does not tell us that P is true, so the truth of the second statement provides no information on the truth of the original statement.

Below is a correct proof that shows that each side of the equality to be proved is equal to the same value.

Since $z_1 = 1+2i$, we have

$$\begin{aligned}|z_1| &= \sqrt{1^2+2^2}\\ &= \sqrt{5}\,.\end{aligned}$$

Since $z_2 = \sqrt{3} - i\sqrt{2}$, we have

$$\begin{aligned}|z_2| &= \sqrt{\left(\sqrt{3}\right)^2 + \left(-\sqrt{2}\right)^2}\\ &= \sqrt{3+2}\\ &= \sqrt{5}.\end{aligned}$$

Therefore $|z_1| = \sqrt{5}$ and $|z_2| = \sqrt{5}$, so $|z_1| = |z_2|$ as required.

(An alternative, but less obvious, proof starts with the left-hand side of the equality to be proved and shows directly that it is equal to the right-hand side.

$$\begin{aligned}|z_1| &= \sqrt{1^2+2^2}\\ &= \sqrt{5}\\ &= \sqrt{3+2}\\ &= \sqrt{\left(\sqrt{3}\right)^2 + \left(-\sqrt{2}\right)^2}\\ &= |z_2|.\end{aligned}$$

Therefore $|z_1| = |z_2|$, as required.)

Solution to Exercise A113

(a) Assume that n is even. Then $n = 2k$ for some integer k, and so

$$\begin{aligned}n+8 &= 2k+8\\ &= 2(k+4).\end{aligned}$$

Since $k+4$ is an integer, this shows that $n+8$ is even. So

$$n \text{ is even} \implies n+8 \text{ is even}.$$

Now assume that $n+8$ is even. Then $n+8 = 2k$ for some integer k, and so

$$\begin{aligned}n &= 2k-8\\ &= 2(k-4).\end{aligned}$$

Since $k-4$ is an integer, this shows that n is even. So

$$n+8 \text{ is even} \implies n \text{ is even}.$$

Hence n is even $\iff$ $n+8$ is even.

(b) Assume that $A \subseteq A \cap B$, and let x be such that $x \in A$. Since $A \subseteq A \cap B$, it follows that $x \in A \cap B$, so, in particular, $x \in B$. Therefore $A \subseteq B$. So

$$A \subseteq A \cap B \implies A \subseteq B.$$

Now assume that $A \subseteq B$, and let x be such that $x \in A$. Then, since $A \subseteq B$, it follows that $x \in B$, and so $x \in A \cap B$. Hence $A \subseteq A \cap B$. So

$$A \subseteq B \implies A \subseteq A \cap B.$$

Hence $A \subseteq A \cap B \iff A \subseteq B$.

Solution to Exercise A114

The initial explanation of how to find a suitable integer is not a necessary part of the solution: it is included to show a possible way to find the example.

The condition $3^n > 9^n$ is equivalent to

$$\frac{3^n}{9^n} = \left(\frac{1}{3}\right)^n > 1.$$

This condition is satisfied by negative values of n, for example $n = -1$.

Let $n = -1$. Then $3^n = \frac{1}{3}$, $9^n = \frac{1}{9}$ and $\frac{1}{3} > \frac{1}{9}$, so $3^n > 9^n$, as required.

Solution to Exercise A115

There are many other possible counterexamples in each part of this exercise.

(a) Taking $m = 1$ and $n = 3$ provides a counterexample since then $m + n = 4$, which is even.

(b) The number -3 is a counterexample because $-3 < 2$ but $((-3)^2 - 2)^2 = (9-2)^2 = 7^2 = 49$, which is not less than 4.

(c) We look for a counterexample. Here is a table for the first few values of n.

n	1	2	3
$4^n + 1$	5	17	65

Since $4^3 + 1 = 65$ is not a prime number, it provides a counterexample, so this implication is false.

Solution to Exercise A116

The implication

$$x^2 = 9 \implies x = 3$$

is false, as $-3 \neq 3$ and $(-3)^2 = 9$, so $x = -3$ is a counterexample. Hence the equivalence is false.

Solution to Exercise A117

(a) Let $P(n)$ be the statement

$$1 + 2 + \cdots + n = \tfrac{1}{2}n(n+1).$$

$P(1)$ is true since $1 = \frac{1}{2}1(1+1)$.

Let $k \geq 1$, and assume that $P(k)$ is true; that is,

$$1 + 2 + \cdots + k = \tfrac{1}{2}k(k+1).$$

We wish to deduce that $P(k+1)$ is true; that is,

$$1 + 2 + \cdots + k + (k+1) = \tfrac{1}{2}(k+1)(k+2).$$

Now

$$\begin{aligned} &1 + 2 + \cdots + k + (k+1) \\ &\quad = \tfrac{1}{2}k(k+1) + (k+1) \quad (\text{by } P(k)) \\ &\quad = (k+1)\left(\tfrac{1}{2}k + 1\right) \\ &\quad = \tfrac{1}{2}(k+1)(k+2). \end{aligned}$$

Thus, for $k = 1, 2, \ldots$,

$$P(k) \implies P(k+1).$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$.

(b) Let $P(n)$ be the statement

$$1^3 + 2^3 + \cdots + n^3 = \tfrac{1}{4}n^2(n+1)^2.$$

$P(1)$ is true since

$$1^3 = 1 \quad \text{and} \quad \tfrac{1}{4}1^2(1+1)^2 = 1.$$

Let $k \geq 1$, and assume that $P(k)$ is true; that is,

$$1^3 + 2^3 + \cdots + k^3 = \tfrac{1}{4}k^2(k+1)^2.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$1^3 + 2^3 + \cdots + k^3 + (k+1)^3 = \tfrac{1}{4}(k+1)^2(k+2)^2.$$

Now

$$\begin{aligned} &1^3 + 2^3 + \cdots + k^3 + (k+1)^3 \\ &\quad = \tfrac{1}{4}k^2(k+1)^2 + (k+1)^3 \quad (\text{by } P(k)) \\ &\quad = (k+1)^2\left(\tfrac{1}{4}k^2 + (k+1)\right) \\ &\quad = \tfrac{1}{4}(k+1)^2(k^2 + 4k + 4) \\ &\quad = \tfrac{1}{4}(k+1)^2(k+2)^2. \end{aligned}$$

Thus, for $k = 1, 2, \ldots$,

$$P(k) \implies P(k+1).$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$.

Solution to Exercise A118

(a) Let $P(n)$ be the statement '$4^{2n-3}+1$ is a multiple of 5'.

$P(2)$ is true because $4^{2\times 2-3}+1 = 4^1+1 = 5$.

Now let $k \geq 2$, and assume that $P(k)$ is true; that is,

$$4^{2k-3}+1 \text{ is a multiple of } 5.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$4^{2(k+1)-3}+1 = 4^{2k-1}+1 \text{ is a multiple of } 5.$$

Now

$$\begin{aligned} 4^{2k-1}+1 &= 4^2 4^{2k-3}+1 \\ &= 16\times 4^{2k-3}+1 \\ &= 15\times 4^{2k-3}+4^{2k-3}+1. \end{aligned}$$

The first term here is a multiple of 5, and $4^{2k-3}+1$ is a multiple of 5, by $P(k)$. Therefore $4^{2k-1}+1$ is a multiple of 5. Hence

$$P(k) \implies P(k+1), \text{ for } k = 2, 3, \ldots.$$

By mathematical induction, it follows that $P(n)$ is true, for $n = 2, 3, \ldots$.

(b) Let $P(n)$ be the statement $5^n < n!$.

$P(12)$ is true because $5^{12} = 2.44\times 10^8$ and $12! = 4.79\times 10^8$, both to three significant figures.

Now let $k \geq 12$, and assume that $P(k)$ is true; that is,

$$5^k < k!.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$5^{(k+1)} < (k+1)!.$$

Now

$$\begin{aligned} 5^{k+1} &= 5\times 5^k \\ &< 5\times k! \quad (\text{by } P(k)) \\ &< (k+1)k! \\ &= (k+1)!, \end{aligned}$$

where we have used the fact that $k \geq 12$, so $k+1 \geq 13 > 5$. Thus we have shown that

$$P(k) \implies P(k+1), \text{ for } k = 12, 13, \ldots.$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 12, 13, \ldots$.

Solution to Exercise A119

Let $P(m)$ be the statement

$$\text{if } a \equiv b \pmod{n}, \text{ then } a^m \equiv b^m \pmod{n}.$$

$P(1)$ is the statement

$$\text{if } a \equiv b \pmod{n}, \text{ then } a \equiv b \pmod{n},$$

which is certainly true.

Assume that $P(k)$ is true; that is, assume that

$$\text{if } a \equiv b \pmod{n}, \text{ then } a^k \equiv b^k \pmod{n}.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$\text{if } a \equiv b \pmod{n}, \text{ then } a^{k+1} \equiv b^{k+1} \pmod{n}.$$

So suppose $a \equiv b \pmod{n}$. Then, by $P(k)$, we know that $a^k \equiv b^k \pmod{n}$.

By the multiplication property of congruences, we have that

$$a^{k+1} \equiv b^{k+1} \pmod{n}.$$

Hence $P(k) \implies P(k+1)$, for $k = 1, 2, \ldots$.

Thus, by mathematical induction, $P(m)$ is true, for $m = 1, 2, \ldots$.

Solution to Exercise A120

The statement of $P(n)$ and the proof of step 1 are correct.

However, the '$=$' sign in the argument

$$2^k+1 \leq 2(2^k+1) = 2\times 3^k \quad (\text{by } P(k))$$

is incorrect: $P(k)$ is an inequality, so we can at best conclude that $2(2^k+1) \leq 2\times 3^k$.

Moreover, even after replacing '$=$' by '$\leq$', all we can deduce is that $2^k+1 \leq 3^{k+1}$, which is not $P(k+1)$.

A correct proof of step 2 is as follows.

Assume $P(k)$; that is, assume that $2^k+1 \leq 3^k$. We want to deduce that $P(k+1)$ is true; that is,

$$2^{k+1}+1 \leq 3^{k+1}.$$

Now

$$\begin{aligned} 2^{k+1}+1 &= 2\times 2^k+1 \\ &= 2\times(2^k+1)-1 \\ &\le 2\times 3^k-1 \quad \text{(by } P(k)\text{)} \\ &\le 3\times 3^k-1 \\ &= 3^{k+1}-1 \\ &\le 3^{k+1}. \end{aligned}$$

It follows that $2^{k+1}+1 \le 3^{k+1}$.

Thus $P(k) \implies P(k+1)$, for $k=1,2,\ldots$.

Hence, by mathematical induction, $P(n)$ is true, for $n=1,2,\ldots$.

Solution to Exercise A121

Suppose that there exists a rational number x such that $x^3=2$. Since x is rational, we can write $x=p/q$, where p and q are coprime positive integers.

Then the equation $x^3=2$ becomes

$$\left(\frac{p}{q}\right)^3=2,$$

that is,

$$p^3=2q^3,$$

which tells us that p^3 must be even. Now, the cube of an odd number, say $2k+1$ for some integer k, is odd because

$$\begin{aligned} (2k+1)^3 &= 8k^3+12k^2+6k+1 \\ &= 2(4k^3+6k^2+3k)+1, \end{aligned}$$

so p must be even, and hence it can be written as $2r$ for some integer r. Then our equation becomes

$$(2r)^3=2q^3,$$

so we have

$$q^3=4r^3.$$

Hence q^3, and therefore q, is also even, so 2 is a common factor of p and q. But p and q were assumed to be coprime, so we have obtained a contradiction.

Therefore there is no rational number x such that $x^3=2$.

(Alternatively, instead of proving that the cube of an odd number is odd, you could use the fact that a positive integer is even if and only if its cube is even, which was proved in Worked Exercise A57.)

Solution to Exercise A122

(a) Suppose that there exist real numbers a and b with $ab > \frac{1}{2}(a^2+b^2)$.

Then $a^2-2ab+b^2<0$; that is, $(a-b)^2<0$. Since a square can never be negative this is a contradiction, so our supposition must be false. Hence there are no such real numbers a and b.

(b) Suppose that there exist integers m and n with $5m+15n=357$.

Since m and n are integers, it follows that the left-hand side of this equation, $5m+15n$, is a multiple of 5. However, the right-hand side of the equation, 357, is not a multiple of 5. This is a contradiction, so our supposition must be false. Hence there are no such integers m and n.

Solution to Exercise A123

Suppose that $n=a+2b$, where a and b are positive real numbers. Suppose also that $a<\frac{1}{2}n$ and $b<\frac{1}{4}n$. Then

$$n=a+2b<\tfrac{1}{2}n+2\left(\tfrac{1}{4}n\right)=n.$$

Thus we have deduced that $n<n$. This contradiction shows that the supposition that $a<\frac{1}{2}n$ and $b<\frac{1}{4}n$ must be false; that is, we must have $a\ge\frac{1}{2}n$ or $b\ge\frac{1}{4}n$.

Solution to Exercise A124

(a) We prove the contrapositive implication, which is

$$n \text{ is even} \implies n^3+2n+1 \text{ is odd.}$$

Suppose that n is even. Then $n=2k$ for some integer k, and so

$$\begin{aligned} n^3+2n+1 &= (2k)^3+2\times 2k+1 \\ &= 8k^3+4k+1 \\ &= 2(4k^3+2k)+1. \end{aligned}$$

Since $4k^3+2k$ is an integer, n^3+2n+1 is odd.

Since the contrapositive is true, the original implication is also true.

(Alternatively, you may have based your proof on the fact, proved in Worked Exercise A57, that a positive integer is even if and only if its cube is even.)

(b) We prove the contrapositive implication, which is

> if at least one of m and n is even, then mn is even.

Suppose that at least one of m and n is even; we can take it to be m (since otherwise we can just interchange m and n). Then $m = 2k$ for some integer k. Hence $mn = 2kn$, which is even.

(c) Let n be an integer that is greater than 1. We prove the contrapositive implication, which is

> if n is not a prime number, then n is divisible by at least one of the primes less than or equal to $\sqrt{n}$.

Suppose that n is not a prime number. Then $n = ab$ for some integers a, b, where $1 < a, b < n$. By the result of Worked Exercise A68, at least one of a and b is less than or equal to $\sqrt{n}$. This number has a prime factor, which must also be less than or equal to $\sqrt{n}$, and this prime factor must also be a factor of n. This proves the required contrapositive implication.

Solution to Exercise A125

We prove the contrapositive implication, which is

> if $A - B \neq \varnothing$, then $A \nsubseteq B$.

Suppose that $A - B \neq \varnothing$. Then there is an element x such that $x \in A$ but $x \notin B$. It follows that $A \nsubseteq B$, as required.

Solution to Exercise A126

The proof is incorrect because it has used the converse of the statement to be proved, rather than its contrapositive. The contrapositive is

> if n is even, then $n^3 + 3$ is odd.

An implication and its converse are not equivalent, therefore the given argument is not a proof of the original statement. Instead, it is a correct proof by contraposition of the implication

> if $n^3 + 3$ is odd, then n is even.

A correct proof of the contrapositive of the original statement is as follows. Suppose n is even. Then $n = 2k$ for some integer k, and therefore

$$\begin{aligned} n^3 + 3 &= (2k)^3 + 3 \\ &= 8k^3 + 3 \\ &= 2(4k^3 + 1) + 1\,. \end{aligned}$$

Since $4k^3 + 1$ is an integer, this shows that $n^3 + 3$ is odd, as required.

Solution to Exercise A127

Statement (b) is false and the other three statements are true.

Solution to Exercise A128

(a) (i) The statement $1.3 \sim 5.3$ is true because $1.3 - 5.3 = -4$ is an integer.

(ii) The statement $2.8 \sim 2.1$ is false because $2.8 - 2.1 = 0.7$ is not an integer.

(iii) The statement $2.4 \sim -5.4$ is false because $2.4 - (-5.4) = 2.4 + 5.4 = 7.8$ is not an integer.

(b) (i) A real number y such that $0.8 \sim y$ is 1.8, for example, since $0.8 - 1.8 = -1$ is an integer.

(ii) A real number z such that $0.8 \not\sim z$ is 0, for example, since $0.8 - 0 = 0.8$ is not an integer.

(There are many other possible solutions to part (b).)

Solution to Exercise A129

(a) E1 The relation 'has sat next to' is not reflexive, since no one has sat next to themself.

E2 However, it is symmetric, because if person A has sat next to person B, then it follows that person B has sat next to person A.

(Here we have assumed that when we say 'A has sat next to B' we mean that A and B have *both* been *sitting* next to each other: we do not allow the possibility that only A sat while B stood, for example.)

E3 Finally, it is not transitive, because if person A has sat next to person B, and person B has sat next to person C, then it does not follow that person A has sat next to person C.

Hence this relation is not an equivalence relation.

(b) E1 The relation 'was born in the same year as' is reflexive, because each person was born in the same year as themself.

E2 It is also symmetric, because if person A was born in the same year as person B, then it follows that person B was born in the same year as person A.

E3 Finally, it is transitive, because if person A was born in the same year as person B, and person B was born in the same year as person C, then person A was born in the same year as person C.

Hence this relation is an equivalence relation.

Solution to Exercise A130

(a) E1 Let $n \in \mathbb{Z}$. Then $n - n = 0$, which is even, so $n \sim n$. Thus $\sim$ is reflexive.

E2 Let $m, n \in \mathbb{Z}$ and suppose that $m \sim n$. Then $m - n$ is even. Since $n - m = -(m - n)$, it follows that $n - m$ is also even. Hence $n \sim m$. Thus $\sim$ is symmetric.

E3 Let $l, m, n \in \mathbb{Z}$ and suppose that $l \sim m$ and $m \sim n$. Then $l - m$ is even and $m - n$ is even. Since the sum of two even numbers is also even, it follows that

$$l - m + m - n = l - n$$

is also even. Hence $l \sim n$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

(b) E1 The relation $\sim$ is not reflexive: for example, we have $2 \not\sim 2$, since $2 - 2 = 0$ which is not odd.

E2 Let $m, n \in \mathbb{Z}$ and suppose that $m \sim n$. Then $m - n$ is odd. Since $n - m = -(m - n)$, it follows that $n - m$ is also odd. Hence $n \sim m$. Thus $\sim$ is symmetric.

E3 The relation $\sim$ is not transitive: for example, $3 \sim 2$ since $3 - 2$ is odd, and $2 \sim 1$ since $2 - 1$ is odd, but $3 \not\sim 1$ since $3 - 1$ is even.

Since $\sim$ is not reflexive (or transitive), it is not an equivalence relation.

(c) E1 Let $n \in \mathbb{Z}$. Then $n^2 + n^2 = 2n^2$, which is even since n^2 is an integer, so $n \sim n$. Thus $\sim$ is reflexive.

E2 Let $m, n \in \mathbb{Z}$ and suppose that $m \sim n$. Then $m^2 + n^2$ is even, and so $n^2 + m^2$ is also even. Hence $n \sim m$. Thus $\sim$ is symmetric.

E3 Let $l, m, n \in \mathbb{Z}$ and suppose that $l \sim m$ and $m \sim n$. Then $l^2 + m^2$ is even and $m^2 + n^2$ is even. Hence

$$l^2 + m^2 = 2j \quad \text{and} \quad m^2 + n^2 = 2k,$$

where $j, k \in \mathbb{Z}$. Hence

$$l^2 = 2j - m^2 \quad \text{and} \quad n^2 = 2k - m^2,$$

so

$$\begin{aligned} l^2 + n^2 &= 2j - m^2 + 2k - m^2 \\ &= 2(j + k - m^2), \end{aligned}$$

which is even, since $j + k - m^2$ is an integer. Hence $l \sim n$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

(d) E1 Let $z \in \mathbb{C}$. Then $|z| = |z|$, so $z \sim z$. Thus $\sim$ is reflexive.

E2 Let $z_1, z_2 \in \mathbb{C}$ and suppose that $z_1 \sim z_2$. Then $|z_1| = |z_2|$, and so $|z_2| = |z_1|$. Hence $z_2 \sim z_1$. Thus $\sim$ is symmetric.

E3 Let $z_1, z_2, z_3 \in \mathbb{C}$ and suppose that $z_1 \sim z_2$ and $z_2 \sim z_3$. Then $|z_1| = |z_2|$ and $|z_2| = |z_3|$. Hence $|z_1| = |z_3|$, that is, $z_1 \sim z_3$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

(e) E1 Let l be a line in the plane. Then l is parallel to itself, so $l \sim l$. Thus $\sim$ is reflexive.

E2 Let l_1 and l_2 be lines in the plane and suppose that $l_1 \sim l_2$. Then l_1 is parallel to l_2, so l_2 is parallel to l_1. That is, $l_2 \sim l_1$. Thus $\sim$ is symmetric.

E3 Let l_1, l_2 and l_3 be lines in the plane and suppose that $l_1 \sim l_2$ and $l_2 \sim l_3$. Then l_1 is parallel to l_2 and l_2 is parallel to l_3. It follows that l_1 is parallel to l_3, that is, $l_1 \sim l_3$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

(f) **E1** Let $x \in \mathbb{R}$. Then $\lfloor x - x \rfloor = \lfloor 0 \rfloor = 0$, so $x \sim x$. Thus $\sim$ is reflexive.

E2 The relation $\sim$ is not symmetric: for example, $0.5 \sim 0$, since

$$\lfloor 0.5 - 0 \rfloor = \lfloor 0.5 \rfloor = 0,$$

but $0 \not\sim 0.5$, since

$$\lfloor 0 - 0.5 \rfloor = \lfloor -0.5 \rfloor = -1 \neq 0.$$

E3 The relation $\sim$ is not transitive: for example, $1 \sim 0.5$, since

$$\lfloor 1 - 0.5 \rfloor = \lfloor 0.5 \rfloor = 0$$

and $0.5 \sim 0$, since

$$\lfloor 0.5 - 0 \rfloor = \lfloor 0.5 \rfloor = 0,$$

but $1 \not\sim 0$, since

$$\lfloor 1 - 0 \rfloor = \lfloor 1 \rfloor = 1 \neq 0.$$

Since $\sim$ is not symmetric (or transitive), it is not an equivalence relation.

Solution to Exercise A131

(a) We start by proving properties E2 (symmetry) and E3 (transitivity) for this relation $\sim$, and then show that property E1 (reflexivity) does not hold.

E2 Let $x, y \in \mathbb{R}$ and suppose that $x \sim y$. Then $xy > 0$, from which it follows that $yx > 0$. Hence $y \sim x$. Thus $\sim$ is symmetric.

E3 Let $x, y, z \in \mathbb{R}$ and suppose that $x \sim y$ and $y \sim z$. Then $xy > 0$ and $yz > 0$. By the first of these inequalities, x and y are either both positive or both negative, and by the second of the inequalities, y and z are either both positive or both negative. It follows that x, y and z are either all positive or all negative. Hence $xz > 0$. Thus $\sim$ is transitive.

E1 The relation $\sim$ is not reflexive; for example, $0 \not\sim 0$, because $0 \times 0 = 0$ which is not greater than 0.

(b) The error in the proof is the statement 'Let y be an element of X such that $x \sim y$'. This statement makes the assumption that there is such an element y, but there may not be.

The argument in the proof is correct apart from this step, so it works for each element x that is related to another element y, but it does not work for an element x that is not related to any other element in the set X. This is why taking $\sim$ to be the relation defined in part (a), and taking $x = 0$, provides a counterexample: for this relation, there is no $y \in \mathbb{R}$ such that $0 \sim y$.

Solution to Exercise A132

We have

$$\begin{aligned}
[\![1]\!] &= \{n \in \mathbb{Z} : 1 \sim n\} \\
&= \{n \in \mathbb{Z} : 1 - n \text{ is even}\} \\
&= \{n \in \mathbb{Z} : 1 - n = 2k \text{ for some integer } k\} \\
&= \{n \in \mathbb{Z} : n = -2k + 1 \text{ for some integer } k\} \\
&= \{n \in \mathbb{Z} : n = 2k + 1 \text{ for some integer } k\} \\
&= \{n \in \mathbb{Z} : n \text{ is odd}\}.
\end{aligned}$$

So $[\![1]\!]$ is the set of odd integers.

Solution to Exercise A133

In Exercise A132 we found that $[\![1]\!]$ is the set of odd integers.

We might suspect that the set of even integers is also an equivalence class. To check this, we can find the equivalence class $[\![0]\!]$. We have

$$\begin{aligned}
[\![0]\!] &= \{n \in \mathbb{Z} : 0 \sim n\} \\
&= \{n \in \mathbb{Z} : 0 - n \text{ is even}\} \\
&= \{n \in \mathbb{Z} : -n = 2k \text{ for some integer } k\} \\
&= \{n \in \mathbb{Z} : n = -2k \text{ for some integer } k\} \\
&= \{n \in \mathbb{Z} : n \text{ is even}\}.
\end{aligned}$$

So, as suspected, $[\![0]\!]$ is the set of even integers.

Since the set of even integers and the set of odd integers form a partition of the set $\mathbb{Z}$, they are the only two equivalence classes of $\sim$.

Solution to Exercise A134

(a) **E1** Let $x \in \mathbb{R}$. Then $\lfloor x \rfloor = \lfloor x \rfloor$, so $x \sim x$. Thus $\sim$ is reflexive.

E2 Let $x, y \in \mathbb{R}$ and suppose that $x \sim y$. Then $\lfloor x \rfloor = \lfloor y \rfloor$, that is, $\lfloor y \rfloor = \lfloor x \rfloor$. Hence $y \sim x$. Thus $\sim$ is symmetric.

E3 Let $x, y, z \in \mathbb{R}$ and suppose that $x \sim y$ and $y \sim z$. Then $\lfloor x \rfloor = \lfloor y \rfloor$ and $\lfloor y \rfloor = \lfloor z \rfloor$. Hence $\lfloor x \rfloor = \lfloor z \rfloor$, that is, $x \sim z$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

(b) We have

$$\begin{aligned}[\![1]\!] &= \{y \in \mathbb{R} : 1 \sim y\} \\ &= \{y \in \mathbb{R} : \lfloor 1 \rfloor = \lfloor y \rfloor\} \\ &= \{y \in \mathbb{R} : 1 = \lfloor y \rfloor\} \\ &= \{y \in \mathbb{R} : \lfloor y \rfloor = 1\} \\ &= [1, 2).\end{aligned}$$

That is, the equivalence class $[\![1]\!]$ is the interval $[1, 2)$.

Similarly, we have

$$\begin{aligned}[\![-4]\!] &= \{y \in \mathbb{R} : -4 \sim y\} \\ &= \{y \in \mathbb{R} : \lfloor -4 \rfloor = \lfloor y \rfloor\} \\ &= \{y \in \mathbb{R} : -4 = \lfloor y \rfloor\} \\ &= \{y \in \mathbb{R} : \lfloor y \rfloor = -4\} \\ &= [-4, -3).\end{aligned}$$

That is, the equivalence class $[\![-4]\!]$ is the interval $[-4, -3)$.

(c) The equivalence classes of $\sim$ are the intervals of the form $[n, n+1)$ where n is an integer. The collection of all such intervals partitions the set $\mathbb{R}$.

Solution to Exercise A135

E1 Let $x \in X$. Then x belongs to the same subset in the partition as itself, so $x \sim x$. Thus $\sim$ is reflexive.

E2 Let $x, y \in X$ and suppose that $x \sim y$. Then x and y belong to the same subset in the partition, so $y \sim x$. Thus $\sim$ is symmetric.

E3 Let $x, y, z \in X$ and suppose that $x \sim y$ and $y \sim z$. Then x and y belong to the same subset in the partition, and y and z belong to the same subset in the partition. It follows that x, y and z all belong to the same subset in the partition, so $x \sim z$. Thus $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

Solution to Exercise A136

Since $4 + 4 = 8$ and the equivalence class $[\![8]\!]$ of congruence modulo 5 contains the element 3 of $\mathbb{Z}_5$, we have $4 +_5 4 = 3$.

Similarly, since $3 \times 4 = 12$ and the equivalence class $[\![12]\!]$ of congruence modulo 5 contains the element 2 of $\mathbb{Z}_5$, we have $3 \times_5 4 = 2$.

Solution to Exercise A137

(a) The solution to Exercise A133 shows that $\sim$ has only two equivalence classes, namely the set of all even integers and the set of all odd integers.

So a suitable set of representatives is the set $\{0, 1\}$.

(There are other choices, of course: any set containing exactly one even integer and exactly one odd integer, such as $\{22, 7\}$ or $\{4, -1\}$, is a set of representatives, but $\{0, 1\}$ (that is, $\mathbb{Z}_2$) is the most natural choice.)

(b) In Exercise A134 it was found that the equivalence classes of $\sim$ are the intervals of the form $[n, n+1)$ where n is an integer.

A suitable set of representatives is $\mathbb{Z}$.

(There are other choices, such as the set $\left\{n + \frac{1}{2} : n \in \mathbb{Z}\right\}$, but $\mathbb{Z}$ is the most natural choice.)

Unit A4

Real functions, graphs and conics

Introduction

In this unit you will look at *real functions* and their *graphs*. The graph of a real function f is the set of points in $\mathbb{R}^2$ with coordinates $(x, f(x))$, where x is in the domain of f.

You will revise some basic real functions and their graphs, and see how some of the properties of these functions are featured in their graphs. You will learn how to apply similar principles to sketch the graphs of more complicated functions, including sums, quotients and composites of other functions, and functions that are defined by different rules for different values of x.

Finally, you will revise *conics*, and see how functions may be used to represent curves in the plane even when the curves themselves are *not* the graphs of functions.

Familiarity with basic calculus is assumed throughout this unit.

1 Real functions and their graphs

In this section you will revise a wide variety of real functions, and look at their graphs and some of their properties.

1.1 Real functions

In Unit A1 *Sets, functions and vectors*, you saw that a **real function** is a function whose domain and codomain are both subsets of $\mathbb{R}$. For example, the following are real functions:

$$\begin{aligned} f : [0,2] &\longrightarrow \mathbb{R} \\ x &\longmapsto 2x-5 \end{aligned} \qquad \text{and} \qquad \begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2. \end{aligned}$$

It is important to remember that a real function, like any function, consists of three things: a domain, a codomain and a rule. It does not consist solely of a rule. In this unit, we usually refer to a real function simply as a 'function', unless there is a reason to emphasise that it is a real function.

The notation used above can be a little unwieldy when used frequently, so we often simplify it by adopting certain conventions. For example, we usually write the function f above as

$$f(x) = 2x-5 \quad (x \in [0,2]).$$

This type of notation specifies the rule and the domain of a function. It does not specify the codomain, but we use the convention that the codomain of a real function is $\mathbb{R}$ unless otherwise stated.

If we do not want to give a function a name, such as f, then we can specify it by giving its rule and domain in the following manner:

$$x \longmapsto 2x-5 \quad (x \in [0,2]).$$

As well as omitting the codomain when we specify a real function, we can sometimes simplify further by omitting the domain too, and stating just the rule. For example, we might specify the function g above by writing simply

$$g(x) = x^2.$$

When we do this, we use the following convention.

Convention for real functions

When a real function is specified *only by a rule*, it is understood that the domain of the function is the set of all real numbers for which the rule is applicable, and the codomain of the function is $\mathbb{R}$.

For example, the function specified only by the rule

$$f(x) = \frac{1}{\sqrt{4 - x^2}}$$

does not have domain $\mathbb{R}$, because the square root here is a real number only when $4 - x^2 \geq 0$; that is, when $x^2 \leq 4$. This is true when x satisfies the inequalities $-2 \leq x \leq 2$ and for no other values of x. Furthermore, we cannot divide by 0, so we must exclude the values -2 and 2 from the domain. Thus the domain of f is the interval $(-2, 2)$.

Exercise A138

For each of the following rules, determine the domain of the corresponding real function f.

(a) $x \longmapsto \dfrac{1}{1 - x^2}$ (b) $x \longmapsto 4x^3 - 3x^2 - 6x + 4$

(c) $x \longmapsto \dfrac{x^2 - 5x + 4}{x^2 + 5x + 4}$ (d) $x \longmapsto \dfrac{1}{\sqrt{1 - x^2}}$

It can sometimes be useful to specify the domain of a real function as a union of the intervals on which it is defined. For example, the function $f(x) = 1/x$ has domain $\mathbb{R}^* = \mathbb{R} - \{0\}$, which can be rewritten in terms of a union of intervals as $(-\infty, 0) \cup (0, \infty)$.

Exercise A139

For each of the functions in Exercise A138, write down the interval, or union of intervals, on which the function is defined.

1.2 Graphs of basic functions

In this subsection we briefly review various families of basic real functions whose graphs you need to be able to recognise and sketch quickly. You should have met most of these functions in your previous studies.

Remember that a *sketch* of the graph of a function is not intended to achieve the detail possible with a computer plot: instead, it should provide a visual summary of the main properties of the function.

Constant functions

The simplest family of functions is the family of **constant functions**, that is, functions of the form $f(x) = b$, where b is a real number. The graph of the function $f(x) = b$ is a horizontal line with y-intercept b, as illustrated in Figure 1.

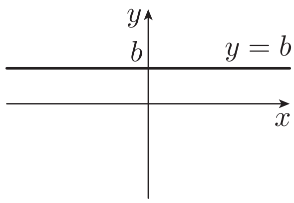


Figure 1 The graph of a constant function

Linear functions

The next simplest family is the family of **linear functions**, that is, functions of the form $f(x) = ax + b$, where $a, b \in \mathbb{R}$ and $a \neq 0$. The graph of the linear function $f(x) = ax + b$ is the straight line with gradient a and y-intercept b, as illustrated in Figure 2(a). In particular, if $b = 0$, so that the function is of the form $f(x) = ax$, then its graph is the straight line through the origin with gradient a, as illustrated in Figure 2(b).

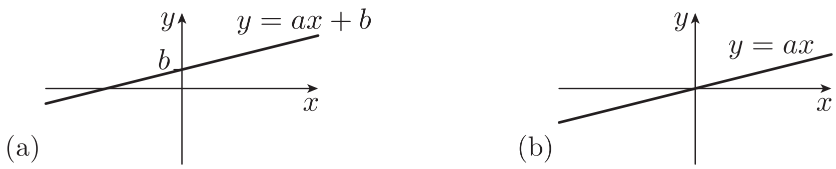


Figure 2 Graphs of linear functions

If a is positive, then the line slopes up as x increases; if a is negative, then it slopes down. It is straightforward to draw the graph of a linear function: you simply plot any two points on the graph and draw a straight line through them.

Quadratic functions

A **quadratic function** is a function of the form $f(x) = ax^2 + bx + c$, where $a, b, c \in \mathbb{R}$ and $a \neq 0$. The simplest quadratic function is the function $f(x) = x^2$, whose graph is shown in Figure 3(a). The graph of every quadratic function has a symmetrical 'cup' shape, called a **parabola**, which is either the same way up as the graph of $f(x) = x^2$ or the other way up, as shown in Figure 3(b). This figure also reminds you what is meant by the **vertex** and the **axis** of a parabola.

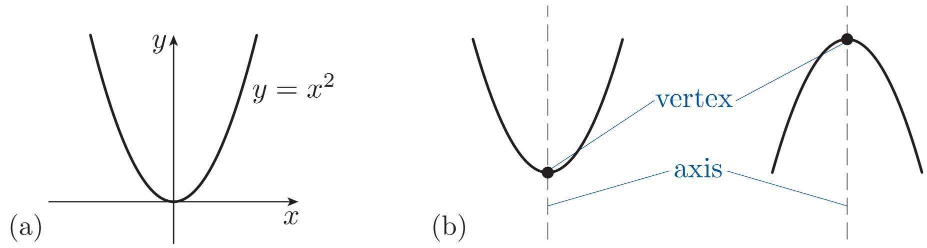


Figure 3 Parabolas

One way to sketch the graph of a quadratic function $f(x) = ax^2 + bx + c$ is to first rearrange the expression $ax^2 + bx + c$ into **completed-square form** (the next worked exercise reminds you how to do this).

After we have completed the square, a quadratic function has the form

$$f(x) = a\,(x - \alpha)^2 + \beta,$$

where a is the same number as in the original expression, and α and β are numbers (which can be positive, negative or zero) that depend on the values of a, b and c. The vertex of the parabola is the point (α, β), as illustrated in Figure 4, and the parabola is the same way up as the graph of $f(x) = x^2$ if $a > 0$, and the opposite way up if $a < 0$. The larger the magnitude of a, the steeper the parabola.

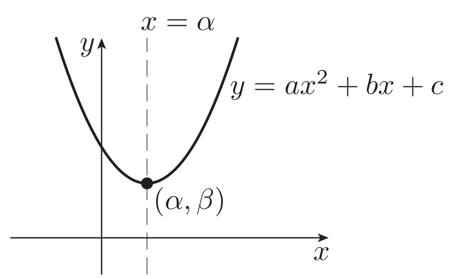


Figure 4 The graph of a quadratic function

Worked Exercise A77

By completing the square, find the vertex of the parabola that is the graph of the function $f(x) = 3x^2 - 2x - 1$.

Solution

Take a, the coefficient of x^2, out as a common factor from the terms in x^2 and x.

$$\begin{aligned} f(x) &= 3x^2 - 2x - 1 \\ &= 3\left(x^2 - \tfrac{2}{3}x\right) - 1 \end{aligned}$$

Write the quadratic expression in the brackets in the form $(x+s)^2 - s^2$. The required value of s is half of the coefficient of x in the brackets.

$$\begin{aligned} &= 3\left((x - \tfrac{1}{3})^2 - (-\tfrac{1}{3})^2\right) - 1 \\ &= 3\left((x - \tfrac{1}{3})^2 - \tfrac{1}{9}\right) - 1 \end{aligned}$$

Multiply out the *outer* brackets, then collect the constant terms.

$$\begin{aligned} &= 3\left(x - \tfrac{1}{3}\right)^2 - \tfrac{1}{3} - 1 \\ &= 3\left(x - \tfrac{1}{3}\right)^2 - \tfrac{4}{3}. \end{aligned}$$

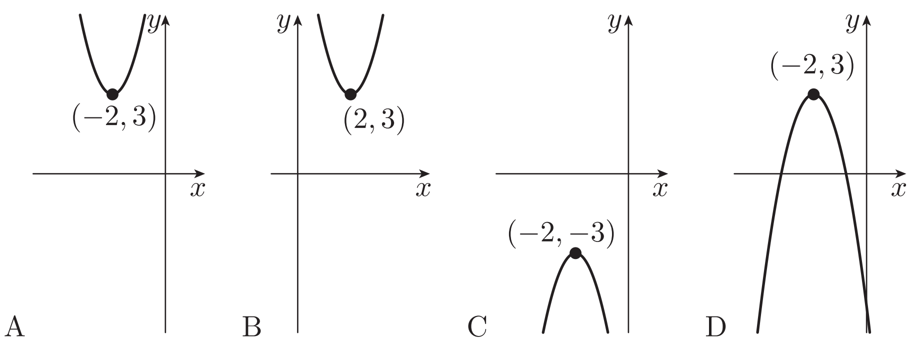
This expression is in completed-square form. The vertex is $\left(\frac{1}{3}, -\frac{4}{3}\right)$.

Exercise A140

Match each of the following quadratic functions to its graph, by first completing the square in each case.

(a) $f(x) = 2x^2 - 8x + 11$ (b) $f(x) = -2x^2 - 8x - 5$

(c) $f(x) = -2x^2 - 8x - 11$ (d) $f(x) = 2x^2 + 8x + 11$



Cubic functions

A **cubic function** is a function of the form $f(x) = ax^3 + bx^2 + cx + d$, where $a \neq 0$. The simplest cubic function is the function $f(x) = x^3$, whose graph is shown in Figure 5(a). This graph has rotational symmetry because the graph is unchanged by rotation through an angle π about the origin; that is, rotating the part of the graph that corresponds to positive values of x through π radians about the origin gives the part of the graph that corresponds to negative values of x.

However, there is more than one basic shape for the graph of a cubic function. Figures 5(b)–(d) show three more examples of such graphs, which illustrate the following features.

- The graph of a cubic function $f(x) = ax^3 + bx^2 + cx + d$ crosses the x-axis once or three times, or (more rarely) crosses it once and 'touches' it once.
- If $a > 0$, then the graph is positive for large positive values of x and negative for large negative values of x.
- If $a < 0$, then the graph is negative for large positive values of x and positive for large negative values of x.

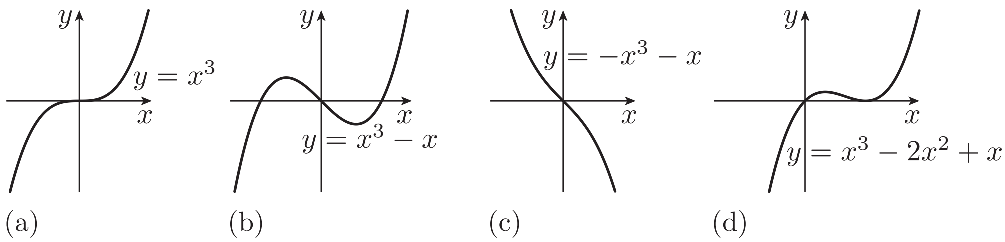


Figure 5 Graphs of cubic functions

Linear rational functions

A **linear rational function** is a function of the form

$$f(x) = \frac{ax + b}{cx + d},$$

where $a, b, c, d \in \mathbb{R}$ are such that $c \neq 0$, and a and b are not both 0. Thus the numerator of a linear rational function is either a constant or a linear function, and the denominator is a linear function.

The simplest linear rational function is the function $f(x) = 1/x$, known as the **reciprocal function**, whose graph is shown in Figure 6(a). The graph is in two parts, because the function $f(x) = 1/x$ is not defined when $x = 0$. It has two *asymptotes*, namely the x- and y-axes. Remember that an **asymptote** of a curve is a straight line that the curve approaches arbitrarily closely as the domain variable x or the codomain variable y (or both) take very large values.

In general, the graph of a linear rational function $f(x) = (ax + b)/(cx + d)$ has a shape known as a *rectangular hyperbola*, with a horizontal asymptote $y = a/c$ and a vertical asymptote $x = -d/c$, as illustrated in Figure 6(b).

The horizontal asymptote $y = a/c$ arises because, for large positive and negative values of x, the value of the function is approximately $ax/cx = a/c$. The vertical asymptote $x = -d/c$ arises because the function is undefined when the denominator $cx + d$ is zero.

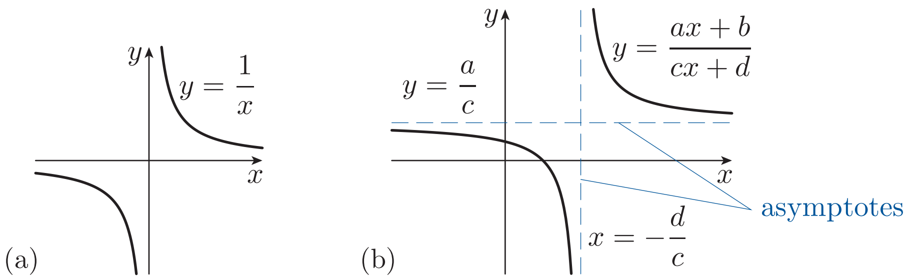


Figure 6 Graphs of linear rational functions

Trigonometric functions

Figure 7 shows the graphs of the trigonometric functions sine and cosine (usually abbreviated as sin and cos). These two graphs are very similar: they both look like waves in a horizontal strip between the lines $y = -1$ and $y = 1$. Each of the two graphs is **periodic** with **period** 2π, which means that the shape of the graph repeats every 2π units on the x-axis, but does not repeat like this at a shorter distance. So, in each graph, the shape in the shaded region of length 2π repeats indefinitely in both directions. The two graphs have exactly the same shape; the cosine graph is obtained by shifting the sine graph to the left by the distance $\pi/2$. The graphs have gradient 1 or -1 where they cross the x-axis.

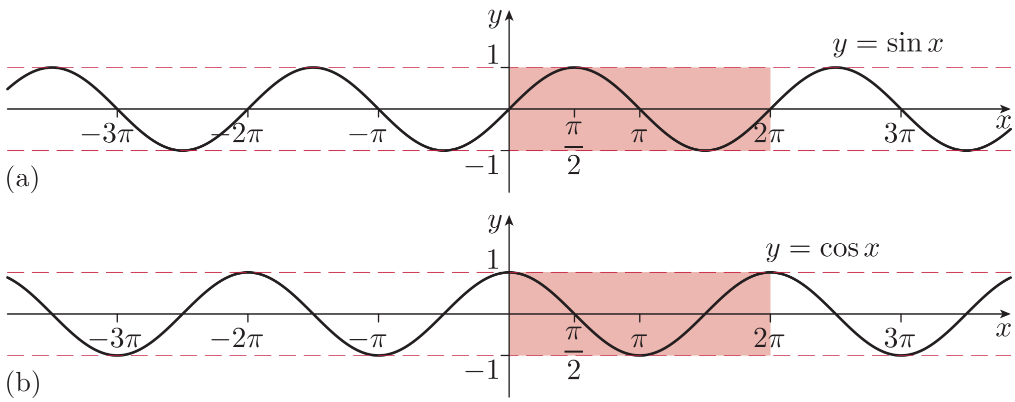


Figure 7 Graphs of (a) sine and (b) cosine

Figure 8 shows the graph of the trigonometric function tangent (tan), which is given by $\tan x = (\sin x)/(\cos x)$. This graph is periodic with period π, so the shape of the graph in the shaded region of length π repeats indefinitely in both directions. The graph has gradient 1 where it crosses the x-axis, and a larger positive gradient at all other points on the graph. The function tan is undefined at each odd multiple of $\pi/2$; that is, at $x = \pm\pi/2$, $\pm 3\pi/2$, $\pm 5\pi/2$, and so on. The graph has a vertical asymptote at each of these values.

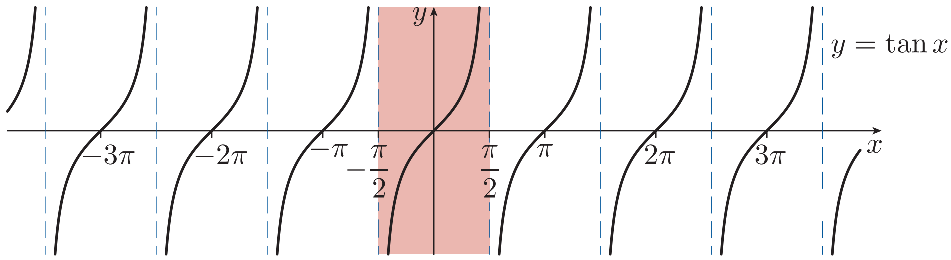


Figure 8 Graph of tan

There are three more standard trigonometric functions, namely cosecant, secant and cotangent (cosec, sec and cot), given by

$$\operatorname{cosec} x = \frac{1}{\sin x}, \quad \sec x = \frac{1}{\cos x} \quad \text{and} \quad \cot x = \frac{\cos x}{\sin x}.$$

You will not often need to sketch the graphs of these functions, but they are included in Figure 9 for completeness.

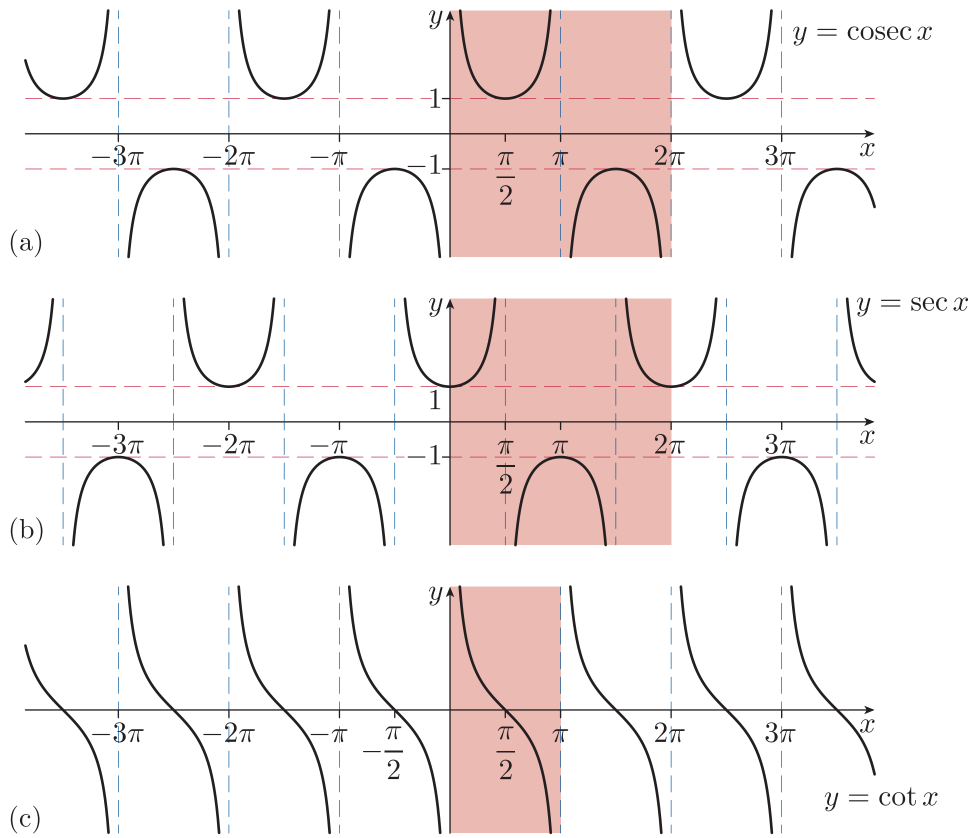


Figure 9 Graphs of (a) cosec, (b) sec and (c) cot

Exponential functions

An **exponential function** is a function of the form $f(x) = a^x$, where a is positive. (In some texts, the trivial case $f(x) = 1^x$, that is, $f(x) = 1$ is not regarded as an exponential function.)

Figure 10(a) illustrates the shape of the graph of an exponential function $f(x) = a^x$ when $a > 1$, and Figure 10(b) illustrates the shape when $0 < a < 1$. An important feature of these graphs is that they lie completely above the x-axis, because a^x is always greater than 0, even when x is negative. One useful point to plot is the point $(0, 1)$, since the graph of an exponential function always passes through this point. This is because $a^0 = 1$ for any positive number a.

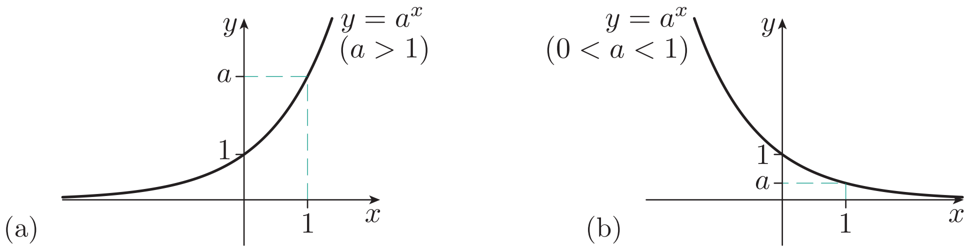


Figure 10 Graphs of exponential functions

Figure 11(a) shows the graph of the special exponential function $f(x) = e^x$, sometimes called ***the* exponential function**. The value e is an irrational number, equal to 2.718 to three decimal places. You will be reminded why e is important later in the module. Figure 11(b) shows the graph of the exponential function $f(x) = (1/e)^x$, more usually written as $f(x) = e^{-x}$.

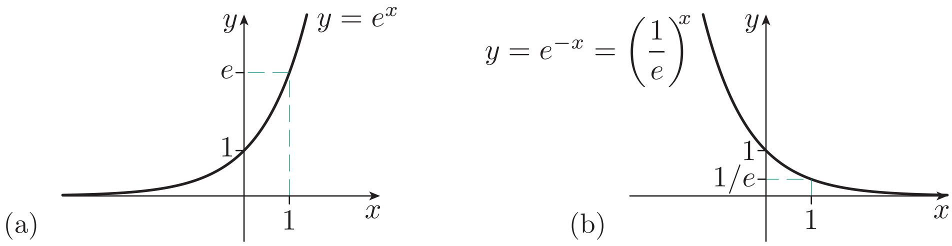


Figure 11 Graphs of exponential functions $f(x) = e^x$ and $f(x) = e^{-x}$

The first known use of the letter e to represent the number 2.718... is in a manuscript written by Leonhard Euler (1707–1783) in 1727 or 1728, although not published until 1862. Euler's first publication to contain e was his *Mechanica* of 1736. It is not known why he chose the letter e, but it is likely that it was because it was the next available letter in the alphabet, earlier letters already being in frequent use in mathematics.

For the functions we have discussed so far in this subsection, the graph takes the form of a smooth curve on each interval in the domain. The next two functions are not so 'well behaved'; their graphs are not smooth curves throughout their domains, because they have either 'corners' or 'jumps'. You will learn more about functions with properties like these in the analysis units of this module.

Modulus function

Figure 12 shows the graph of the **modulus function** $f(x) = |x|$. As you saw in Unit 1, the notation $|x|$, usually read as 'mod x', means the **modulus** (also called **absolute value** or **magnitude**) of the number x, which is given by

$$|x| = \begin{cases} x, & \text{if } x \geq 0, \\ -x, & \text{if } x < 0. \end{cases}$$

For example, $|3| = 3$ and $|-3| = 3$. The graph of $f(x) = |x|$ is the same as the graph of $y = x$ when $x \geq 0$, and the same as the graph of $y = -x$ when $x \leq 0$. It has a corner at the origin.

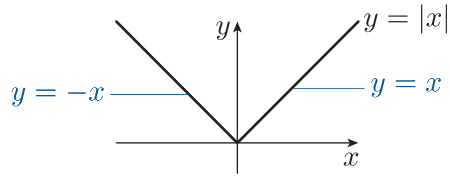


Figure 12 Graph of the modulus function

Integer part function

Figure 13 shows the graph of an even more peculiar function, the **integer part function** $f(x) = \lfloor x \rfloor$. For each x, the **integer part** $\lfloor x \rfloor$ of x is obtained by rounding down to the nearest integer. The rounding is always *down*, no matter whether x is positive or negative. For example,

$$\lfloor 2.8 \rfloor = 2, \quad \lfloor -2.8 \rfloor = -3 \quad \text{and} \quad \lfloor 2 \rfloor = 2.$$

So the graph of $f(x) = \lfloor x \rfloor$ consists of horizontal line segments with jumps between them. The left-hand endpoint of each line segment belongs to the graph, whereas the right-hand endpoint does not. This is indicated on the graph by the solid dot at each left-hand endpoint and the hollow dot at each right-hand endpoint.

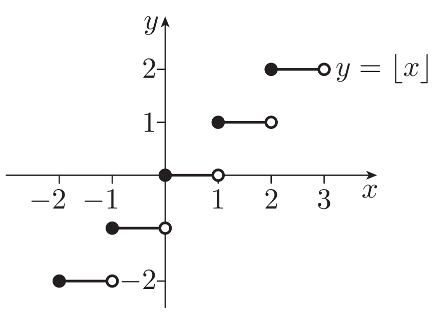


Figure 13 Graph of the integer part function

In some texts, the integer part of a number is denoted by $[x]$ or $\mathrm{Int}(x)$, and sometimes the integer part function is called the **floor function**.

Curves that are not the graphs of functions

If f is a real function with domain A, then f maps each real number x in A to a single real number $f(x)$. That is, each number in the domain has exactly one image. This tells us that if we take the graph of f and draw a vertical line through any number on the x-axis, then that vertical line must cross the graph at most once. It will cross it once if the number on the x-axis is in A, and it will not cross it at all otherwise. So, for example, Figure 14(a) is the graph of a function, whereas Figure 14(b) is not, because the vertical line crosses the curve three times.

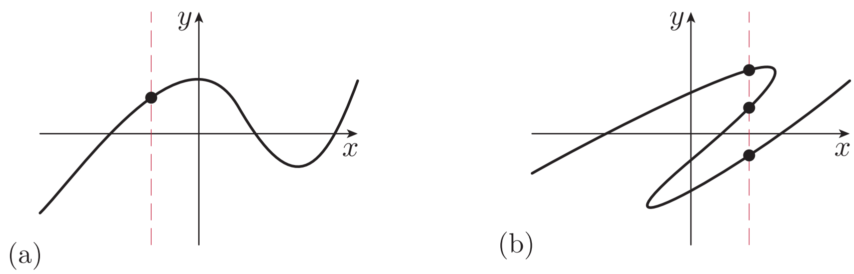


Figure 14 (a) The graph of a function and (b) a curve that is not the graph of a function

Recognising graphs

You should now be able to recognise the graphs of functions that belong to the basic families covered in this subsection, or are related to them in a simple way. You should also be able to recognise curves that are not the graphs of functions.

You can practise this using Figure 15. Each numbered part of the figure shows either

- the graph of $y = f(x)$, where f is a function belonging to, or closely related to, one of the families of functions discussed in this subsection, or
- a curve in the plane that is not the graph of such a function.

For example, here are some comments on the first four parts of Figure 15 to get you started.

- Part 1 is a (non-vertical) straight line, so it is the graph of a linear function.
- Part 2 is cup-shaped, so it is the graph of a quadratic function.
- In part 3, it is possible to draw a vertical straight line that crosses the curve more than once, so this curve is not the graph of y as some function of x.
- Part 4 appears to be the graph of a function related to the modulus function.

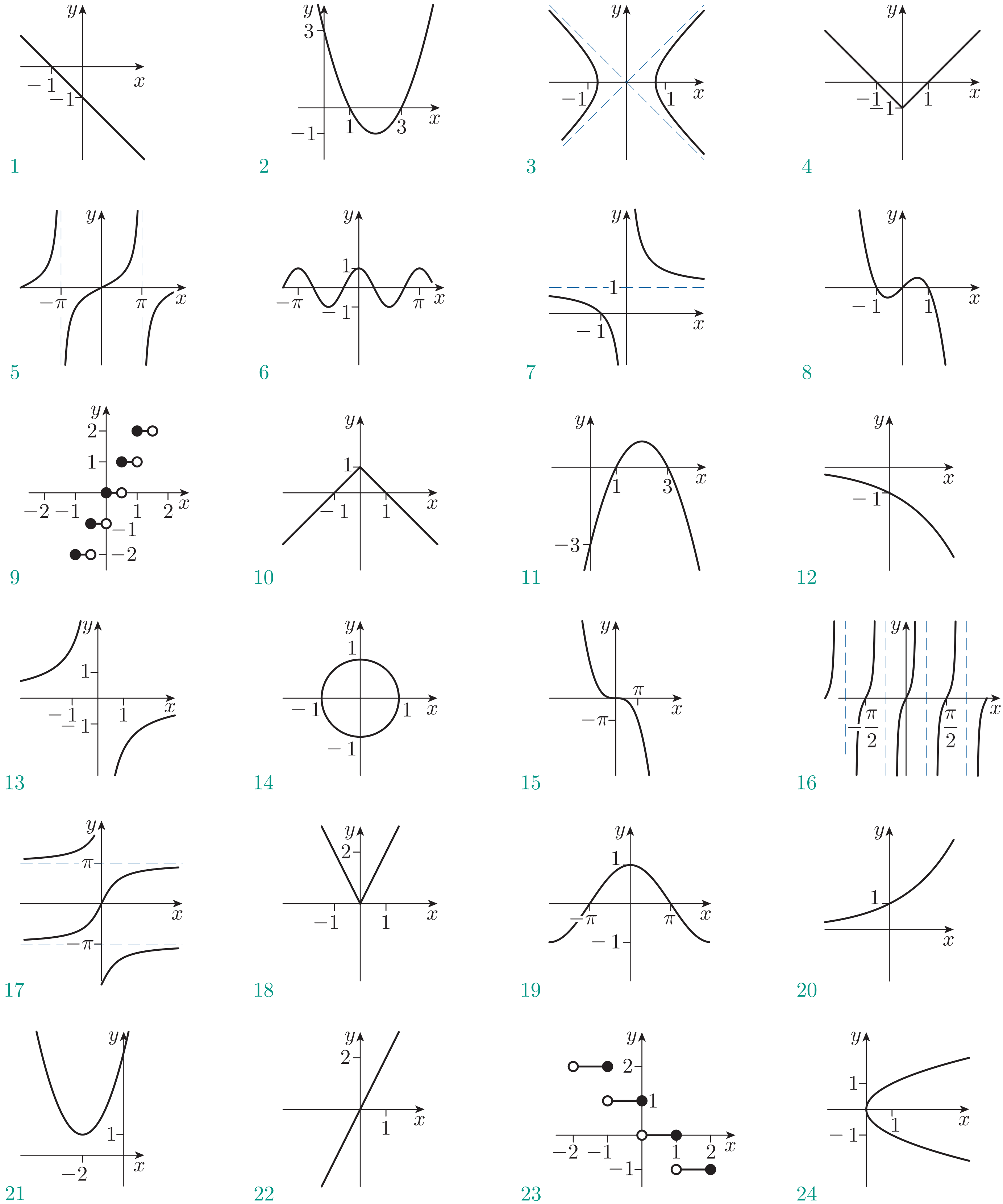


Figure 15 A selection of graphs and curves

The next exercise asks you to classify each of the parts of Figure 15 in a similar way.

Exercise A141

Look through all of the numbered parts of Figure 15, fairly quickly, and try to decide which of the following families each belongs to.

(a) Linear

(b) Quadratic

(c) Cubic

(d) Trigonometric

(e) Linear rational

(f) Modulus (or related)

(g) Integer part (or related)

(h) Exponential (or related)

(i) Not the graph of y as some function of x.

1.3 Translations and scalings of graphs

In this subsection we will revise some simple transformations that can be applied to graphs, and the effects that these transformations have on the rules of the corresponding functions. Knowing about these transformations allows you to recognise and sketch the graphs of a wide variety of functions related to those discussed in the previous subsection, and to understand some of the properties of such functions.

Translations

Figure 16 shows the graph of a function $y = f(x)$, and the graph obtained by translating it by α units to the right and β units upwards. This transformation is called an (α, β)-**translation**.

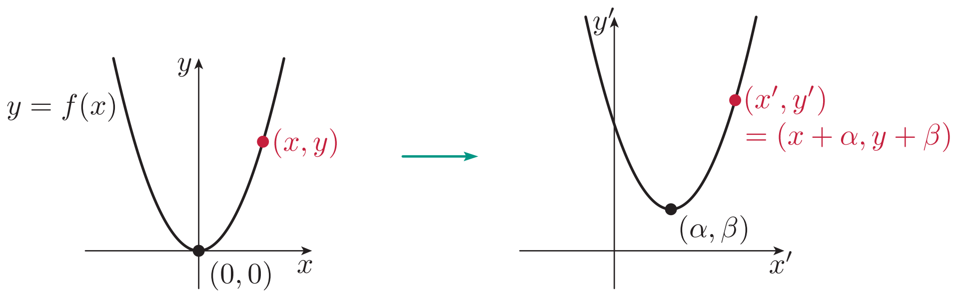


Figure 16 The effect of an (α, β)-translation

Let us determine the equation of the translated graph. To do this, it is helpful to temporarily use different symbols to denote the coordinates of points on the translated graph. Let us use x' and y', as shown on the axes of the translated graph in Figure 16. Now consider any point (x', y') on the translated graph. We want to determine the relationship between x' and y'. The point (x', y') on the translated graph is obtained by translating some point, say (x, y), on the original graph, so $x' = x + \alpha$ and $y' = y + \beta$, that is,

$$x = x' - \alpha \quad \text{and} \quad y = y' - \beta. \tag{1}$$

We know that the relationship between the coordinates x and y of the point (x, y) on the original graph is given by the equation $y = f(x)$. Using equations (1) to substitute into this equation gives

$$y' - \beta = f(x' - \alpha).$$

This equation gives the relationship between the coordinates x' and y' of the point (x', y') on the translated graph. If we now rearrange it to obtain just y' on the left-hand side, and use the usual x and y rather than x' and y' for the coordinates on the translated graph, then we obtain

$$y = f(x - \alpha) + \beta.$$

So this is the equation of the translated graph. For example, if the original graph has equation $y = x^2$, and the translation is a $(3, 2)$-translation, then the equation of the translated graph is $y = (x - 3)^2 + 2$. This quadratic expression, in its completed-square form, is $y = a(x - \alpha)^2 + \beta$ so, by the result you met in Subsection 1.2, its vertex is at $(\alpha, \beta) = (3, 2)$. This is just what we would expect, because $(3, 2)$ is the image of the origin under a $(3, 2)$-translation.

The values α and β in an (α, β)-translation can be positive, zero or negative. A negative value of α gives a translation to the left rather than to the right, and a negative value of β gives a translation downwards rather than upwards.

Scalings

Figure 17 shows the graph of a function $y = f(x)$, and the graph obtained by scaling (stretching) it by the factor λ in the x-direction and the factor μ in the y-direction, where $\lambda, \mu \neq 0$. This transformation is called a (λ, μ)-**scaling**.

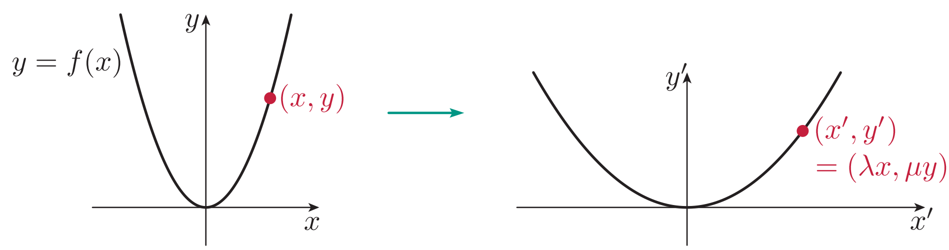


Figure 17 The effect of a (λ, μ)-scaling

Let us determine the equation of the scaled graph. To do this, as before we use x' and y' to denote the coordinates of points on the scaled graph, as shown in Figure 17. Now consider any point (x', y') on the scaled graph. It is obtained from some point, say (x, y), on the original graph, where $x' = \lambda x$ and $y' = \mu y$, that is,

$$x = \frac{x'}{\lambda} \quad \text{and} \quad y = \frac{y'}{\mu}. \tag{2}$$

We know that the relationship between the coordinates x and y of the point (x, y) is given by the equation $y = f(x)$. Using equations (2) to substitute into this equation gives

$$\frac{y'}{\mu} = f\left(\frac{x'}{\lambda}\right).$$

This equation gives the relationship between the coordinates x' and y' of the point (x', y') on the scaled graph. If we now rearrange it to obtain just y' on the left-hand side, and use x and y rather than x' and y' for the coordinates, then we obtain

$$y = \mu f\left(\frac{x}{\lambda}\right).$$

So this is the equation of the scaled graph. For example, if the original graph has equation $y = x^2$, and the scaling is a $(2, 1)$-scaling, then the equation of the scaled graph is $y = 1(x/2)^2$, which simplifies to $y = x^2/4$.

If the magnitude of λ, the scale factor in the x-direction, is less than 1, then the graph 'gets closer' to the y-axis, and if the magnitude of λ is greater than 1, then the graph 'gets further away' from the y-axis. A negative value of λ causes the graph to be reflected in the y-axis as well as scaled. These facts also hold for μ, the scale factor in the y-direction, with respect to the x-axis rather than the y-axis.

Applying the transformations

Here is a summary of the results about translations and scalings that you have seen in this subsection.

Translations and scalings of graphs

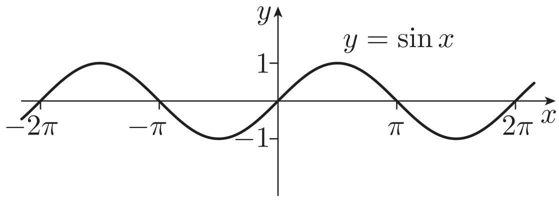
- Applying an (α, β)-translation to the graph of $y = f(x)$ gives the graph of
$$y = f(x - \alpha) + \beta.$$
- Applying a (λ, μ)-scaling to the graph of $y = f(x)$ gives the graph of
$$y = \mu f\left(\frac{x}{\lambda}\right).$$

You might find it easier to appreciate what is happening with these translations and scalings from the following forms of these equations:

$$y - \beta = f(x - \alpha) \quad \text{and} \quad \frac{y}{\mu} = f\left(\frac{x}{\lambda}\right).$$

Worked Exercise A78

The graph of $y = \sin x$ is shown below.



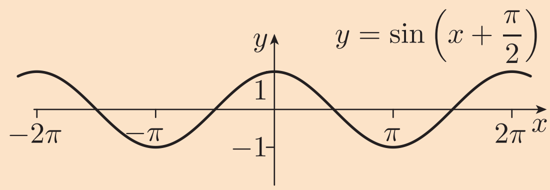
Sketch the graphs of the following.

(a) $y = \sin\left(x + \dfrac{\pi}{2}\right)$ (b) $y = 2\sin x$ (c) $y = \sin 2x$

Solution

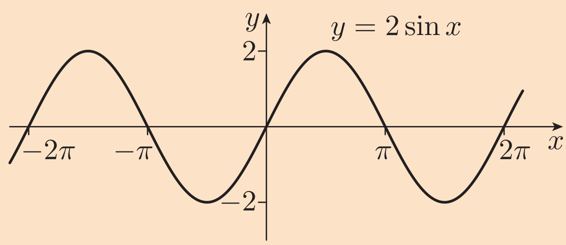
(a) Starting from the equation $y = \sin x$, we replace x by $x + \pi/2$ to obtain the equation $y = \sin(x + \pi/2)$. So we have a translation with $\alpha = -\pi/2$ and $\beta = 0$; that is, a translation to the left by $\pi/2$.

The graph of $y = \sin\left(x + \dfrac{\pi}{2}\right)$ is obtained from the graph of $y = \sin x$ by a $\left(-\dfrac{\pi}{2}, 0\right)$-translation.



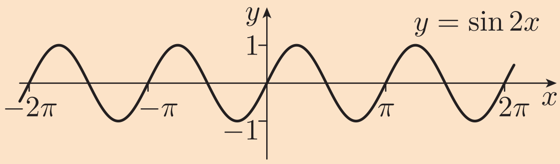
(b) Starting from the equation $y = \sin x$, we multiply the right-hand side by 2 to obtain the equation $y = 2\sin x$. So we have a scaling with $\lambda = 1$ and $\mu = 2$; that is, a scaling by a factor of 2 vertically.

The graph of $y = 2\sin x$ is obtained from the graph of $y = \sin x$ by a $(1, 2)$-scaling.



(c) Starting from the equation $y = \sin x$, we multiply x by 2 to obtain the equation $y = \sin 2x$. So we have a scaling with $\lambda = 1/2$ and $\mu = 1$; that is, a scaling by a factor of a half horizontally.

The graph of $y = \sin 2x$ is obtained from the graph of $y = \sin x$ by a $\left(\frac{1}{2}, 1\right)$-scaling.



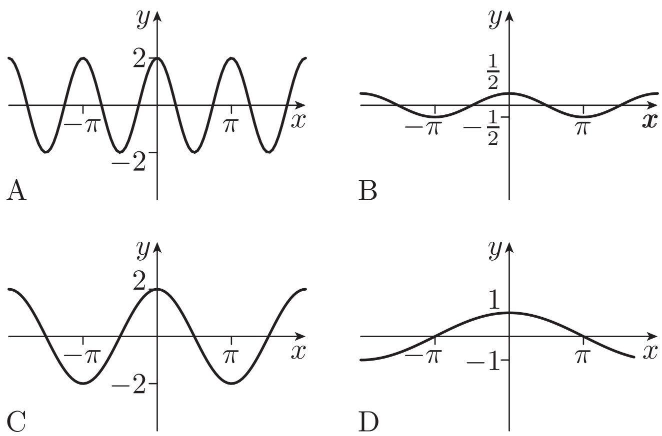
Since the graph of $y = \sin\left(x + \dfrac{\pi}{2}\right)$, as shown in the solution to Worked Exercise A78(a), is obtained by translating the graph of $y = \sin x$ to the left by the distance $\pi/2$, it is the same as the graph of $y = \cos x$. In other words, $\cos x = \sin\left(x + \dfrac{\pi}{2}\right)$ for each real number x.

Exercise A142

Determine how the graph of each of the following trigonometric functions can be obtained by transforming the graph of $y = \cos x$, and hence match each function to its graph.

(a) $y = \cos\left(\dfrac{x}{2}\right)$ (b) $y = 2\cos x$ (c) $y = 2\cos 2x$

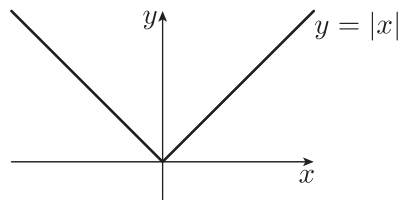
(d) $y = \frac{1}{2}\cos x$



Each of the graphs in Worked Exercise A78 and Exercise A142 involved either a scaling or a translation. The graph in the next worked exercise involves both.

Worked Exercise A79

The graph of $y = |x|$ is shown below.



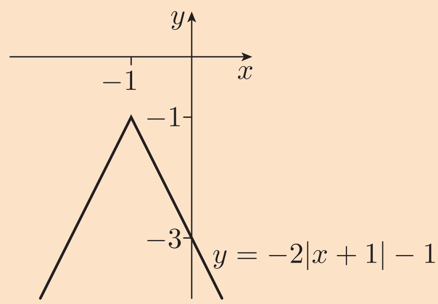
Sketch the graph of $y = -2|x+1| - 1$.

Solution

Here we have both a scaling and a translation, so we have to take care with the order in which we apply them. To do this, we think about how the equation $y = -2|x+1| - 1$ is obtained from the equation $y = |x|$, and apply the corresponding transformations to the graph in the same order.

Starting with the equation $y = |x|$, we multiply the right-hand side by -2 to obtain the equation $y = -2|x|$. We then replace x by $x+1$ in this equation to obtain $y = -2|x+1|$, and finally we add -1.

So the graph of $y = -2|x+1| - 1$ is obtained from the graph of $y = |x|$ by applying a $(1, -2)$-scaling followed by a $(-1, -1)$-translation, which gives the graph sketched below.

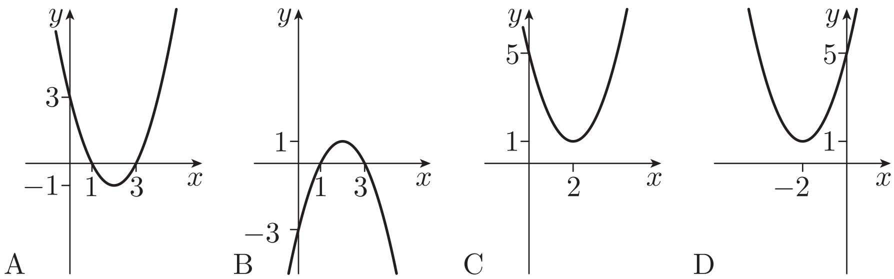


Exercise A143

Determine how the graph of each of the following quadratic functions can be obtained by transforming the graph of $y = x^2$, and hence match each function to its graph.

(a) $y = (x-2)^2 + 1$ (b) $y = (x+2)^2 + 1$ (c) $y = -(x-2)^2 + 1$

(d) $y = (x-2)^2 - 1$



2 Graph sketching

In this section you will be sketching the graphs of functions that are rather more complicated than the basic functions you met in the previous section.

Remember that the aim of sketching the graph of a function is to provide a visual summary of the main properties of the function. Here you will learn techniques for analysing the properties of functions, and see how these techniques can be combined into a general strategy for sketching their graphs.

To begin our investigation of the main properties of functions, let us look carefully at the graph of the function

$$f(x) = \frac{1}{1 - x^2}.$$

By our convention, the domain of this function is the set of all real numbers excluding 1 and -1; its graph is sketched in Figure 18.

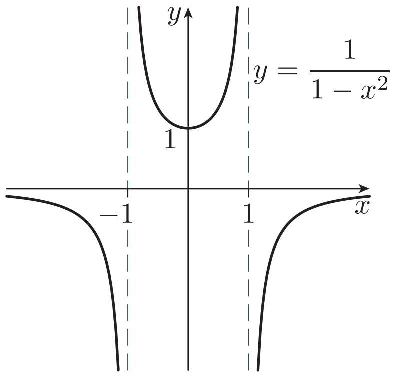


Figure 18 The graph of $y = 1/(1-x^2)$

Several key properties of the function f can be seen from this graph.

- The function is undefined at $x = 1$ and at $x = -1$; that is, its domain consists of the three intervals

  $$(-\infty, -1),\ (-1, 1) \text{ and } (1, \infty).$$

- The graph is symmetric about the y-axis.
- The graph of f crosses the y-axis when $y = f(0) = 1$;
  The graph of f does not cross the x-axis.
- f takes positive values on the interval $(-1, 1)$;
  f takes negative values on the intervals $(-\infty, -1)$ and $(1, \infty)$.
- $f(x)$ increases as x increases on the intervals $(0, 1)$ and $(1, \infty)$;
  $f(x)$ decreases as x increases on the intervals $(-\infty, -1)$ and $(-1, 0)$;
  f has a local minimum at $x = 0$.
- $f(x)$ becomes very large and positive as x approaches 1 from the left or -1 from the right;
  $f(x)$ becomes very large and negative as x approaches 1 from the right or -1 from the left;
  $f(x)$ gets closer and closer to 0 as x becomes large and positive or large and negative.

When sketching the graph of a function, you should concentrate on representing important features like those listed above, since it is these features that help us understand the behaviour of functions. There is no need for a sketch to have the detailed accuracy of a computer plot.

2.1 Determining features of a graph

In this subsection we look in detail at each of the features you saw above in the graph of the function $f(x) = 1/(1 - x^2)$, and discuss how these and related properties arise in the graphs of other functions.

We will consider the properties and graphs of a wide range of functions, including general *polynomial* and *rational* functions. Recall that a **polynomial function of degree** n is a function of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_n \neq 0$. The linear, quadratic and cubic functions you met in Subsection 1.2 are examples of polynomial functions of degree 1, 2 and 3, respectively. A **rational function** is a function defined by a rule of the form

$$x \longmapsto \frac{p(x)}{q(x)},$$

where both p and q are polynomial functions. The linear rational functions you met in Subsection 1.2 are a simple example of this type of function.

We now discuss each of the main features of graphs of functions in turn.

Domain

When the domain of a function is not given, we use our convention and take the domain to be the set of all real numbers for which the given rule is applicable. So the domain is the set of all real numbers, excluding any numbers that give an expression that is not defined – for example, they might make the denominator of a rational function equal to zero, or give a negative number under a square root sign.

When sketching a graph it is particularly helpful to express the domain of a function as a union of intervals, since this emphasises the intervals on which the function is defined, and identifies any points at which it is not defined. For example, you saw above that the function $f(x) = 1/(1 - x^2)$ is defined on the three intervals $(-\infty, -1)$, $(-1, 1)$ and $(1, \infty)$ but is undefined at $x = \pm 1$.

Symmetry features

There are three distinct ways in which the graph of a real function may exhibit symmetry properties. These are illustrated in Figure 19.

- The graph in Figure 19(a) is unchanged when reflected in the y-axis. A function whose graph has this property is called an **even** function.
- The graph in Figure 19(b) is unchanged when rotated through the angle π about the origin. A function whose graph has this property is called an **odd** function.
- The graph in Figure 19(c) is unchanged when translated along the x-axis by a distance p, but not when translated by any distance less than p. A function whose graph has this property is called a **periodic** function with period p.

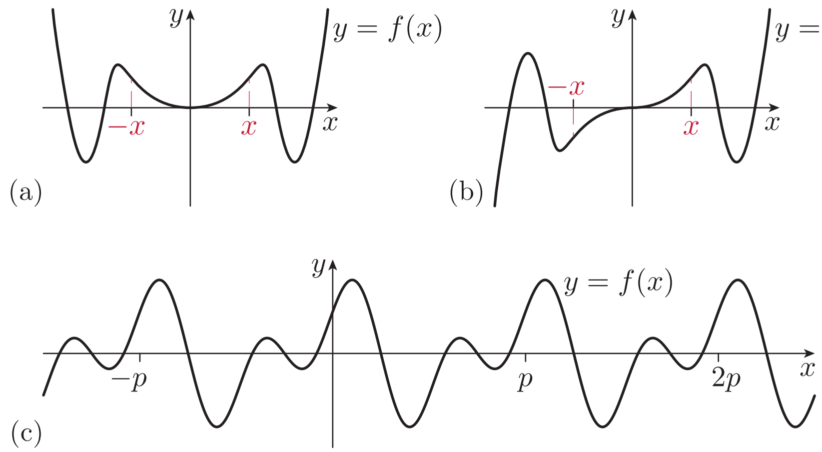


Figure 19 Graphs of (a) an even function, (b) an odd function and (c) a periodic function

These properties can be expressed algebraically as follows.

A function f is **even** if

$$f(-x) = f(x), \quad \text{for all } x \text{ in the domain of } f.$$

A function f is **odd** if

$$f(-x) = -f(x), \quad \text{for all } x \text{ in the domain of } f.$$

A function f is **periodic** if there is a number p such that

$$f(x+p) = f(x), \quad \text{for all } x \text{ in the domain of } f.$$

The markings of x and $-x$ on the x-axes in Figure 19(a) and (b) should help you see why the algebraic definitions of even and odd functions are correct. Notice that the domain of a function must be symmetric about 0 for the concepts of evenness and oddness to make sense.

You have met several examples of even and odd functions already. For example, the functions $x \longmapsto x^2$ and $x \longmapsto \cos x$, whose graphs are shown in Figure 20(a) and (b), are even functions. The function

$f(x) = 1/(1 - x^2)$, whose graph we looked at earlier in this section, is also an even function.

The functions $x \longmapsto x^3$ and $x \longmapsto \sin x$, whose graphs are shown in Figure 20(c) and (d), are odd functions. Note that both even and odd functions may also be periodic; this is true of $x \longmapsto \cos x$ and $x \longmapsto \sin x$, for example.

Many functions are neither odd nor even. To show algebraically that a function is neither odd nor even, we just need to find one value of x in the domain such that $f(-x)$ is equal to neither $-f(x)$ nor $f(x)$.

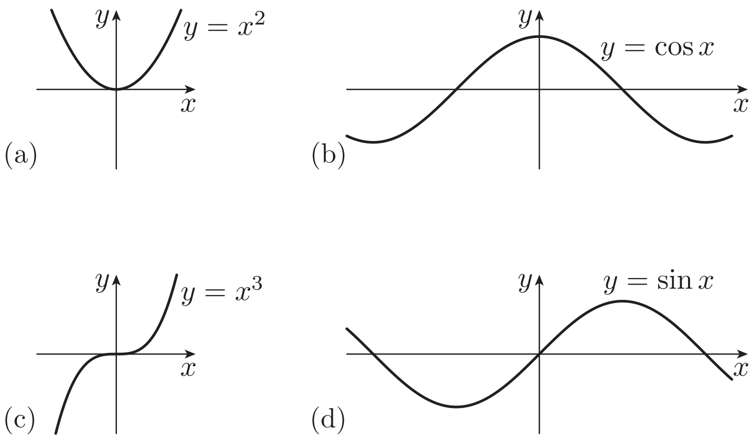


Figure 20 Graphs of (a), (b) even functions and (c), (d) odd functions

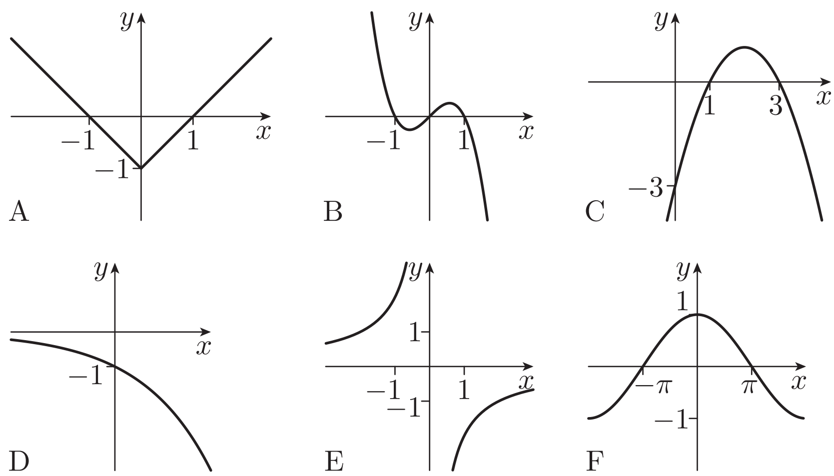
Exercise A144

Identify which of the following is the graph of:

(a) an odd function

(b) an even function

(c) a function that is neither odd nor even.



Intercepts

An **intercept** is a value of x or y at which the graph $y = f(x)$ of a function f meets the x- or y-axis, respectively. The x-intercepts are the solutions (if there are any) of the equation $f(x) = 0$. The y-intercept is the value $f(0)$, if this exists. These features are illustrated in Figure 21.

It is usually straightforward to find the y-intercept, but harder to find the x-intercepts, since this involves solving the equation $f(x) = 0$. It is not always possible to solve this equation algebraically, but it is usually possible to obtain estimates for the solutions by finding intervals of the domain in which the values of the function f change sign.

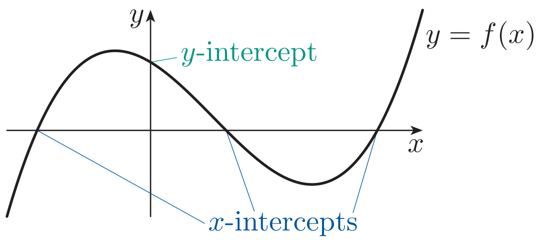


Figure 21 The x-intercepts and the y-intercept of a function f

Intervals on which a function is positive or negative

We say that a function f is **positive** on a particular interval I if $f(x)$ is positive for each value of x in I. So f is positive on the intervals for which the graph lies above the x-axis. For example, the function whose graph is shown in Figure 22(a) is positive on the open intervals (a, b) and (c, ∞). The modulus function, whose graph is shown in Figure 22(b), is positive on the open intervals $(-\infty, 0)$ and $(0, \infty)$.

Similarly, we say that a function f is **negative** on a particular interval I if $f(x)$ is negative for each value of x in I. So f is negative on the intervals for which the graph lies below the x-axis. For example, the function whose graph is shown in Figure 22(a) is negative on the open intervals $(-\infty, a)$ and (b, c). The modulus function is nowhere negative.

We say that a function f has a **zero** at x if $f(x) = 0$. So a function has a zero at each number x where its graph crosses or touches the x-axis, that is, at each of the x-intercepts of f. The function whose graph is Figure 22(a) has zeros at a, b and c, and the modulus function has just one zero, at 0.

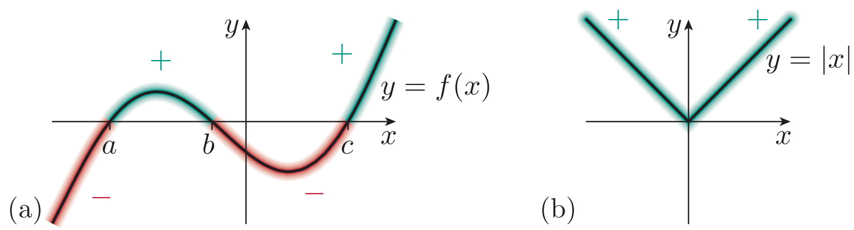


Figure 22 Sections of graphs where a function is positive or negative

If f is a *polynomial* or a *rational* function, a useful technique for finding the intervals on which f is positive or negative is to construct a **table of signs** for f. For example, consider again the rational function

$$f(x) = \frac{1}{1-x^2},$$

whose graph we looked at earlier. We can factorise f as

$$f(x) = \frac{1}{(1-x)(1+x)},$$

and construct the table of signs as follows.

- Write each of the factors of f as the heading of a row in the table, and add a final row for the function $f(x)$ itself. Include any factors from the numerator of a rational function, as well as from the denominator (in this example, the numerator is just 1).
- For the column headings, write (in increasing order) the values of x for which the factors of f are equal to zero, and also the largest open intervals to the left and right of, and between, these values.

For our function f, this gives the following blank table:

x	$(-\infty,-1)$	-1	$(-1,1)$	1	$(1,\infty)$
1					
$1-x$					
$1+x$					
$f(x)$					

Now, for each factor, we complete the table by writing 0, + or − to indicate whether the factor is zero, positive or negative for values of x in the range indicated by each column heading. Finally, in each column, we then use the signs of the factors to determine the sign of f. (Where f is undefined, we enter the symbol $*$ to indicate this.) The resulting table of signs for f is as follows:

x	$(-\infty,-1)$	-1	$(-1,1)$	1	$(1,\infty)$
1	$+$	$+$	$+$	$+$	$+$
$1-x$	$+$	$+$	$+$	0	$-$
$1+x$	$-$	0	$+$	$+$	$+$
$f(x)$	$-$	$*$	$+$	$*$	$-$

From this table of signs we deduce that

- f has no zeros
- f is positive on the interval $(-1,1)$
- f is negative on the intervals $(-\infty,-1)$ and $(1,\infty)$.

If f is a *quadratic* function, and we are unable to factorise it, then we can sometimes find out whether it always has the same sign by completing the square, using the method you saw in Worked Exercise A77. For example,

$$\begin{aligned}2x^2 + 12x + 19 &= 2(x^2 + 6x) + 19\\ &= 2\left((x+3)^2 - 9\right) + 19\\ &= 2(x+3)^2 - 18 + 19\\ &= 2(x+3)^2 + 1.\end{aligned}$$

From this we can see that $2x^2 + 12x + 19$ is always positive, whatever the value of x.

Exercise A145

For each of the following quadratic expressions, complete the square and determine whether it always has the same sign, regardless of the value of x.

(a) $x^2 - 6x + 11$ (b) $3x^2 + 12x - 1$

Intervals on which a function is increasing or decreasing

Look at Figure 23(a), which shows the graph of the integer part function. This graph looks like a staircase: it goes uphill in a sequence of steps. It never goes downhill: as x increases, the value of $f(x)$ either stays the same or gets larger. In this module we say that a function with this property on a particular interval is **increasing** on that interval. So the integer part function is increasing on $\mathbb{R}$. There is an analogous definition of **decreasing**.

Now look at the graph in Figure 23(b), which has no flat sections. On the interval $(-\infty, d)$, the graph goes uphill: $f(x)$ gets larger as x gets larger. So f is increasing on this interval. Moreover, on this interval $f(x)$ increases in the usual sense of the word 'increase'. If we wish to emphasise this, then we say that f is **strictly increasing** on $(-\infty, d)$. On the interval (d, e), the graph goes downhill with no flat sections, and we say that f is **strictly decreasing** on this interval. Finally, on the interval (e, ∞), the graph goes uphill again, so f is strictly increasing on this interval.

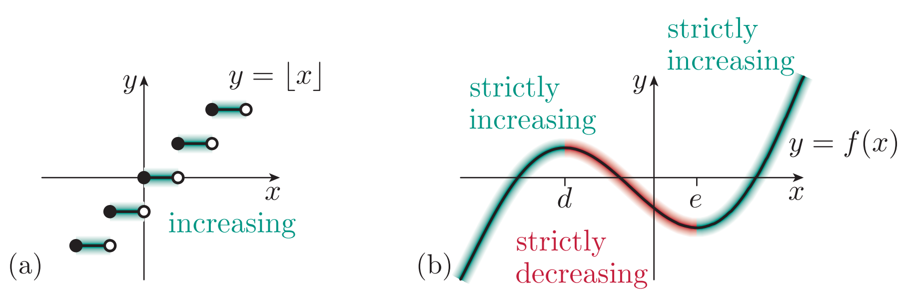


Figure 23 Sections of graphs where a function is increasing or decreasing

Note that, according to our definitions, a function that is strictly increasing on an interval is also increasing on that interval, and similarly a function that is strictly decreasing on an interval is also decreasing on that interval.

Exercise A146

Identify which of the following is the graph of a function that is:

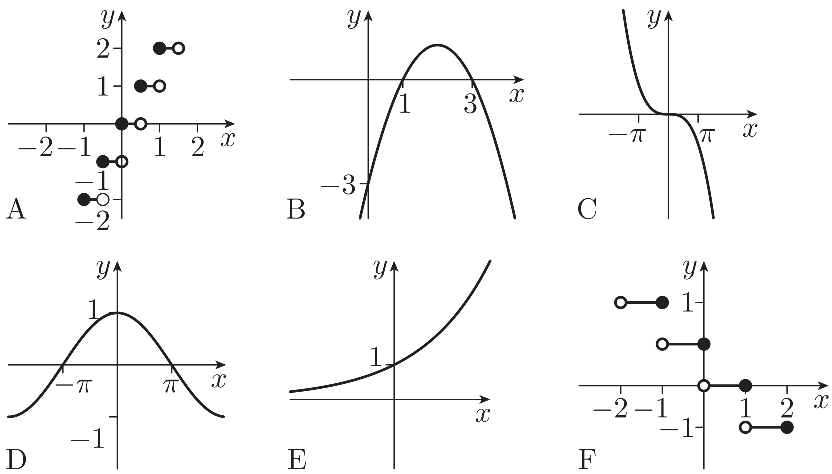
(a) increasing but not strictly increasing

(b) strictly increasing

(c) decreasing but not strictly decreasing

(d) strictly decreasing

(e) increasing on part of its domain and decreasing on another part of its domain.



The following is a formal statement of the definitions introduced in the discussion above.

Definitions

A function f is **increasing** on an interval I, if for all $x_1, x_2 \in I$,

$$\text{if } x_1 < x_2, \quad \text{then } f(x_1) \leq f(x_2).$$

A function f is **strictly increasing** on an interval I, if for all $x_1, x_2 \in I$,

$$\text{if } x_1 < x_2, \quad \text{then } f(x_1) < f(x_2).$$

A function f is **decreasing** on an interval I, if for all $x_1, x_2 \in I$,

$$\text{if } x_1 < x_2, \quad \text{then } f(x_1) \geq f(x_2).$$

A function f is **strictly decreasing** on an interval I, if for all $x_1, x_2 \in I$,

$$\text{if } x_1 < x_2, \quad \text{then } f(x_1) > f(x_2).$$

For a differentiable function f, we can use the derivative f' of the function to identify these intervals. You will meet more formally what it means for a function to be *differentiable* in the analysis units of this module. For the moment, you can assume that a function whose graph has no jumps or sharp corners is differentiable, and that you can find the derivative of the function by the usual methods of calculus. You will find a table of standard derivatives in the module Handbook, and also a list of the rules for differentiating functions that you have met in your previous studies.

Since $f'(x)$ is the gradient of the graph of f at the value x in the domain, we have the following facts.

Increasing/decreasing criteria

- If $f'(x) > 0$ for all x in an interval I, then f is strictly increasing on I.
- If $f'(x) < 0$ for all x in an interval I, then f is strictly decreasing on I.

A point where the graph of a function changes from being strictly increasing to strictly decreasing is called a **local maximum**, because at such a point the value of the function is larger than at all nearby points. Similarly, a point where a graph changes from being strictly decreasing to strictly increasing is called a **local minimum**. For a differentiable function f, these are examples of **stationary points** of the function, that is, values of x at which $f'(x) = 0$. (The term stationary point is sometimes also used to refer to the corresponding point $(x, f(x))$ on the graph of f. The tangent to the graph at such a point is horizontal.)

For example, Figure 24(a) shows the graph of a differentiable function with a local maximum and a local minimum. We see that, for this function,

- if $x \in (-\infty, d)$ or $x \in (e, \infty)$, then $f'(x) > 0$ and f is strictly increasing
- if $x \in (d, e)$, then $f'(x) < 0$ and f is strictly decreasing
- $f'(d) = 0$, and at $x = d$ the graph of f changes from being strictly increasing to strictly decreasing, so f has a local maximum
- $f'(e) = 0$, and at $x = e$ the graph of f changes from being strictly decreasing to strictly increasing, so f has a local minimum.

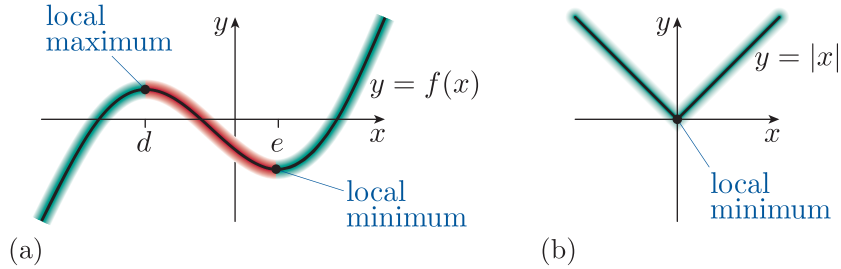


Figure 24 Local maxima and local minima of functions

Note that functions that are not differentiable can still have local maxima or minima. For example, the graph of the modulus function, shown in Figure 24(b), has a local minimum at $x = 0$. For such functions, the local maxima or minima may need to be found without using calculus.

A stationary point of a differentiable function need not be a local maximum or a local minimum. For example, consider $f(x) = x^3$, graphed in Figure 25. Since $f'(0) = 0$, this function has a stationary point at 0, but it has neither a local maximum nor a local minimum there. In fact, it has what we call a *horizontal point of inflection* at $x = 0$.

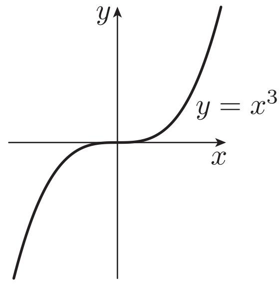


Figure 25 The graph of $f(x) = x^3$

We can check whether a stationary point is a local maximum, a local minimum or a horizontal point of inflection by using the following test.

First Derivative Test

Suppose that a is a stationary point of a differentiable function f, so that $f'(a) = 0$.

- If f' changes from positive to negative as x increases through a, then f has a **local maximum** at a.
- If f' changes from negative to positive as x increases through a, then f has a **local minimum** at a.
- If f' remains positive or remains negative as x increases through a (except at a itself, where $f'(a) = 0$), then f has a **horizontal point of inflection** at a.

Note, however, that f' may do none of these things; for example, a constant function has $f'(x) = 0$ at all values x in the domain, so every point on its graph is a stationary point.

If f is a *polynomial* or a *rational* function, we can construct a **table of signs** for f' to determine the intervals on which f is increasing and decreasing, and at the same time determine the nature of any stationary points. We illustrate this by returning to the function

$$f(x) = \frac{1}{1 - x^2}.$$

To find the intervals on which this function is increasing or decreasing, we use the quotient rule to differentiate f, which gives

$$\begin{aligned} f'(x) &= \frac{(1 - x^2) \times 0 - 1 \times (-2x)}{(1 - x^2)^2} \\ &= \frac{2x}{(1 - x^2)^2}. \end{aligned}$$

There is no need to factorise the term $(1 - x^2)^2$, because its value is always at least 0.

The table of signs for f' is as follows.

x	$(-\infty,-1)$	-1	$(-1,0)$	0	$(0,1)$	1	$(1,\infty)$
$2x$	$-$	$-$	$-$	0	$+$	$+$	$+$
$(1-x^2)^2$	$+$	0	$+$	$+$	$+$	0	$+$
$f'(x)$	$-$	$*$	$-$	0	$+$	$*$	$+$

We find that

- f has a stationary point at 0
- f is increasing on the intervals $(0,1)$ and $(1,\infty)$
- f is decreasing on the intervals $(-\infty,-1)$ and $(-1,0)$.

We deduce that f has a local minimum at 0, by the First Derivative Test.

Exercise A147

Use a table of signs to find the intervals on which the function

$$f(x) = x^4 - 2x^2 + 3$$

is increasing and decreasing, and use the First Derivative Test to determine the nature of the stationary points. Give the value of the function at each of the stationary points.

Asymptotic behaviour of functions

For a function f, the term **asymptotic behaviour** refers to the behaviour of the graph of $y = f(x)$ at the points of the graph for which the variable x or the variable y takes arbitrarily large values.

For example, let us consider how to determine the features of the graph of the function $f(x) = 1/(1-x^2)$ as x or y approaches ∞.

Figure 26(a) shows a plot produced by a computer that has used a 'join-the-dots' approach to generate the graph of this function. The computer plot is inaccurate near the 'missing' points $x = 1$ and $x = -1$, since it gives the impression that the graph is a vertical line at $x = 1$ and $x = -1$, whereas we know that the function is not defined at these points. It is common for computer plots of graphs to give misleading results near such 'difficult' points. By contrast, Figure 26(b) shows a sketch of this graph which indicates the behaviour of the function f near the points 1 and -1 by the use of broken vertical lines.

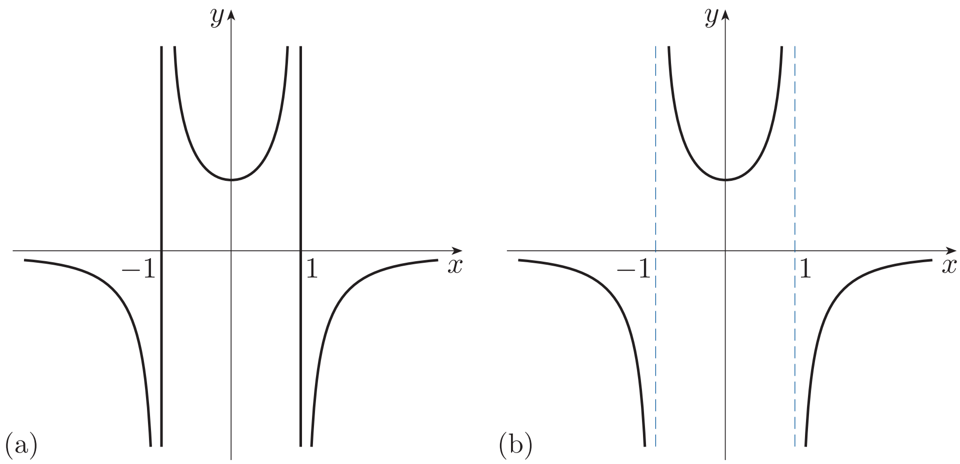


Figure 26 Depictions of the graph of the function $f(x) = 1/(1 - x^2)$ (a) an inaccurate computer plot and (b) a more accurate sketch showing asymptotes

An asymptote with an equation of the form $x = a$ is a **vertical asymptote**. For example, in the graph in Figure 26(b), the lines $x = -1$ and $x = 1$ are vertical asymptotes.

An asymptote with an equation of the form $y = b$ is a **horizontal asymptote**. For example, in the graph in Figure 26(b), the line $y = 0$ is a horizontal asymptote.

A broken line is used to indicate an asymptote on the graph of a function, except when the asymptote coincides with one of the axes. Both features are shown in Figure 26(b), which has two vertical asymptotes, shown as broken lines, and a horizontal asymptote that coincides with the x-axis.

The behaviour of a function f near a vertical asymptote $x = a$ may take various forms. For the example above, we can describe the behaviour near the vertical asymptote $x = -1$ by saying that f takes arbitrarily large positive values as x tends to -1 from the right, which is written in symbols as

$$f(x) \to \infty, \quad \text{as } x \to -1^+,$$

and read as

f of x tends to infinity as x tends to -1 from the right.

Similarly, $f(x)$ takes arbitrarily large negative values as x tends to -1 from the left, which is written in symbols as

$$f(x) \to -\infty, \quad \text{as } x \to -1^-,$$

and read as

f of x tends to minus infinity as x tends to -1 from the left.

You will see how intuitive statements of this nature can be formally defined in Book F *Analysis 2* of this module.

Two more examples of asymptotic behaviour are illustrated in Figure 27.

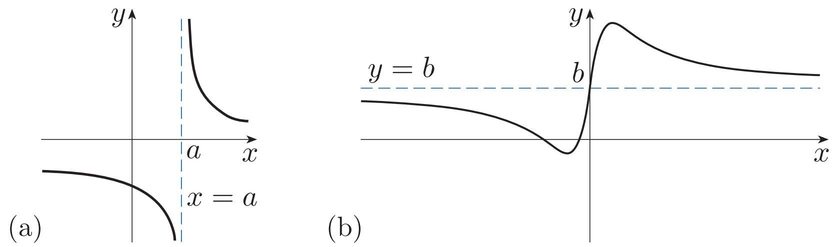


Figure 27 Asymptotic behaviour: (a) vertical asymptote and (b) horizontal asymptote

Figure 27(a) shows a vertical asymptote where

$$f(x) \to \infty, \quad \text{as } x \to a^+ \quad \text{and} \quad f(x) \to -\infty, \quad \text{as } x \to a^-,$$

and Figure 27(b) shows a horizontal asymptote where

$$f(x) \to b, \quad \text{as } x \to \infty \quad \text{and} \quad f(x) \to b, \quad \text{as } x \to -\infty.$$

Figure 27(b) also shows that the graph of a function may cross a *horizontal* asymptote.

Exercise A148

Describe in symbols the behaviour of the function

$$f(x) = \frac{1}{1 - x^2}$$

near the vertical asymptote at $x = 1$ and near the horizontal asymptote.

There are other types of behaviour that a function may exhibit as the domain variable x takes large positive or negative values. For example, the function graphed in Figure 28(a) has

$$f(x) \to \infty, \quad \text{as } x \to \infty \quad \text{and} \quad f(x) \to -\infty, \quad \text{as } x \to -\infty,$$

and the function in Figure 28(b) has

$$f(x) \to -\infty, \quad \text{as } x \to \infty \quad \text{and} \quad f(x) \to \infty, \quad \text{as } x \to -\infty.$$

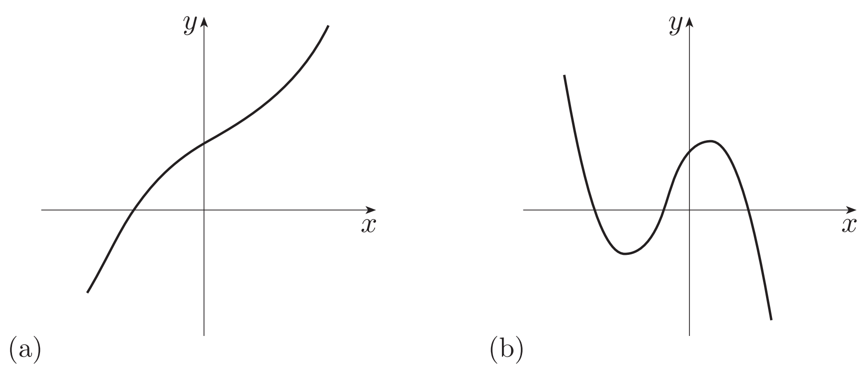


Figure 28 Some other types of asymptotic behaviour

For a function, such as $f(x) = x^2$, where we have

$$f(x) \to \infty, \quad \text{as } x \to \infty \quad \text{and} \quad f(x) \to \infty, \quad \text{as } x \to -\infty,$$

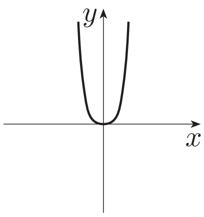
we write

$$f(x) \to \infty, \quad \text{as } x \to \pm\infty.$$

Exercise A149

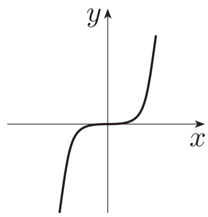
Describe in symbols the asymptotic behaviour of the functions whose graphs are given below.

(a)



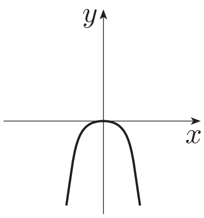
$f(x) = 3x^4$

(b)



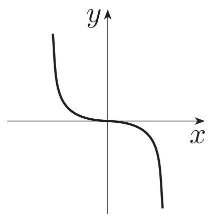
$f(x) = 3x^5$

(c)



$f(x) = -2x^4$

(d)



$f(x) = -2x^5$

If f is a *polynomial* function of degree n, that is, is a function of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_n \neq 0$, then we define the **dominant term** of f to be $a_n x^n$, the term with the highest power of x, and we call a_n the **coefficient** of the dominant term. For example, the polynomial function $f(x) = 4x^3 - 2x^2 + 1$ has dominant term $4x^3$, which has coefficient 4.

A polynomial function f has no vertical asymptotes since it is defined for all x in $\mathbb{R}$, and its asymptotic behaviour for large values of x is the same as that of its dominant term $a_n x^n$. This behaviour is summarised as follows.

$a_n > 0$	$x \to \infty$	$x \to -\infty$
n even	$f(x) \to \infty$	$f(x) \to \infty$
n odd	$f(x) \to \infty$	$f(x) \to -\infty$

$a_n < 0$	$x \to \infty$	$x \to -\infty$
n even	$f(x) \to -\infty$	$f(x) \to -\infty$
n odd	$f(x) \to -\infty$	$f(x) \to \infty$

If f is a *rational function*, that is, a function of the form

$$f(x) = \frac{p(x)}{q(x)},$$

where both p and q are polynomial functions, then locating any vertical and horizontal asymptotes is an important step in sketching its graph.

The *vertical* asymptotes of a rational function occur at the values of x for which $q(x) = 0$ and $p(x) \neq 0$, if there are any such values.

A rational function can have at most one *horizontal* asymptote, and if it does have one, then its graph approaches the asymptote arbitrarily closely as $x \to \pm\infty$.

To find the behaviour of a rational function for large positive or negative values of x, and hence identify any horizontal asymptote, we compare the dominant term of the numerator p, say $a_n x^n$, with the dominant term of the denominator q, say $b_m x^m$:

- if $n > m$, then the rational function has no horizontal asymptote
- if $n < m$, then the line $y = 0$ is a horizontal asymptote
- if $n = m$, then the line $y = c$ is a horizontal asymptote, where c is the ratio of the coefficients of the dominant terms of the numerator and denominator, that is, $c = a_n/b_m$.

You will see this technique applied in the worked exercises in the next subsection.

2.2 Strategy for graph sketching

This subsection begins with a strategy summarising the basic features that a sketch of a graph should convey. This is followed by worked exercises illustrating the strategy, and some exercises for you to try.

Strategy A3 Graph-sketching strategy

To sketch the graph of a function f, determine the following features of f (where possible), and show these features in your sketch.

1. The domain of f.
2. Whether f is even, odd or periodic (or none of these).
3. The x-intercepts and the y-intercept of f, if any.
4. The intervals on which f is positive or negative.
5. The intervals on which f is increasing or decreasing, the nature of any stationary points, and the value of f at each of these points.
6. The asymptotic behaviour of f.

The steps of this strategy are numbered for easy reference, and in this unit are referred to as 'step 1', 'step 2', etc. However, it is not necessary to carry

out the steps in the order given above, although it is important to begin by determining the domain of f. For example, if the domain is $[3, 9]$, then f is neither even nor odd, and you cannot find the behaviour of f as $x \to \infty$.

For some functions, you will be able to obtain enough information to sketch the graph without including all the steps of the strategy. On the other hand, it is often useful to obtain information in more than one way, since this provides a check on your working. For certain functions, though, you may find that some steps in the strategy are not easy to carry out, in which case it is fine to omit them.

One step that is in general quite tricky is testing whether a given function is periodic. All the periodic functions you will meet in this module involve a trigonometric function (sin, cos, tan, cot, sec or cosec), and you need not test for periodicity unless a trigonometric function appears in the rule of f *and* you can guess the period. However, note that not all functions involving a trigonometric function are periodic; this will be the case, for example, if the rule of the function also contains a non-periodic element that 'overrides' the periodic behaviour of the trigonometric function.

When sketching graphs, you should choose the scales on your axes with care: usually, the scales should be the same on both axes, but it may be necessary to have unequal scales in order to display some key features of the graph – for example, when $f(x)$ is much larger than x.

We first use the strategy to sketch the graphs of polynomial functions.

Worked Exercise A80

Sketch the graph of the function

$$f(x) = 4x^3 + 3x^2 - 6x + 4.$$

Solution

1. The domain of f is $\mathbb{R}$. By our convention.
2. There is no trigonometric function involved, so we don't need to consider whether f is periodic – it is not.

   The function is neither even nor odd, since, for example,

   $$f(-1) = 9, \quad \text{but} \quad f(1) = 5.$$

3. Solving $f(x) = 0$, that is, solving $4x^3 + 3x^2 - 6x + 4 = 0$, is not easy since there are no obvious factors, so we try easy values such as $0, \pm 1, \pm 2, \ldots$ to see if f changes sign.

   We have $f(-2) = -4$, and we have already seen in step 2 that $f(-1) = 9$. Thus $f(x)$ changes from negative to positive as x increases from -2 to -1, so there is an x-intercept in the interval $(-2, -1)$. The y-intercept is $f(0) = 4$.

   We have not yet ruled out further x-intercepts.

4. Because we cannot find the zeros of f, we cannot find the intervals on which f is positive or negative.

   By step 3, the sign of f changes from negative to positive as x increases from -2 to -1.

5. Differentiating gives

$$\begin{aligned} f'(x) &= 12x^2 + 6x - 6 \\ &= 6(2x^2 + x - 1) \\ &= 6(2x - 1)(x + 1). \end{aligned}$$

   We construct a table of signs for f'.

x	$(-\infty, -1)$	-1	$\left(-1, \frac{1}{2}\right)$	$\frac{1}{2}$	$\left(\frac{1}{2}, \infty\right)$
$6(2x-1)$	$-$	$-$	$-$	0	$+$
$x+1$	$-$	0	$+$	$+$	$+$
$f'(x)$	$+$	0	$-$	0	$+$

   Thus

   - f is increasing on the intervals $(-\infty, -1)$ and $\left(\frac{1}{2}, \infty\right)$
   - f is decreasing on the interval $\left(-1, \frac{1}{2}\right)$
   - f has stationary points at -1 and $\frac{1}{2}$.

   By the First Derivative Test, we deduce that

   - there is a local maximum at $x = -1$ with $f(-1) = 9$
   - there is a local minimum at $x = \frac{1}{2}$ with $f\left(\frac{1}{2}\right) = \frac{9}{4}$.

   The results of steps 4 and 5 show that the graph of f crosses the x-axis at only one point.

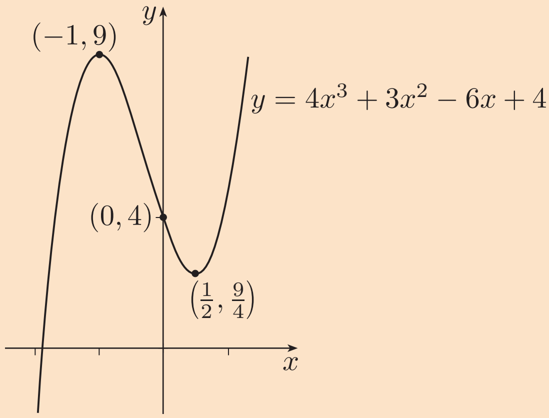
6. We consider the behaviour of the dominant term $4x^3$.

   The power of x in the dominant term is odd and its coefficient is positive, so

$$f(x) \to \infty \text{ as } x \to \infty \quad \text{and} \quad f(x) \to -\infty \text{ as } x \to -\infty.$$

This information enables us to sketch the graph.

Because of the steepness of the curve, it is convenient to use different scales on the x- and y-axes.



Exercise A150

Sketch the graph of the polynomial function

$$f(x) = x^4 - 2x^2 + 3.$$

(You carried out step 5 in Exercise A147.)

Hint: In step 3, if you put $t = x^2$, then the expression becomes $t^2 - 2t + 3$.

Next, we use the strategy to sketch the graphs of linear rational functions.

Worked Exercise A81

Sketch the graph of the function

$$f(x) = \frac{2x - 3}{x - 1}.$$

Solution

1. The domain of f is $\mathbb{R} - \{1\}$. By our convention.
2. The function is neither even nor odd, since its domain is not symmetric about 0.

   Alternatively, $f(-1) = \frac{5}{2}$, but f is not defined at $x = 1$.
3. $f(x) = 0$ when $2x - 3 = 0$, so the x-intercept is $\frac{3}{2}$.

   $f(0) = -3/(-1) = 3$, so the y-intercept is 3.
4. We construct a table of signs for f.

x	$(-\infty, 1)$	1	$\left(1, \frac{3}{2}\right)$	$\frac{3}{2}$	$\left(\frac{3}{2}, \infty\right)$
$2x - 3$	$-$	$-$	$-$	0	$+$
$x - 1$	$-$	0	$+$	$+$	$+$
$f(x)$	$+$	$*$	$-$	0	$+$

So

- f is positive on the intervals $(-\infty, 1)$ and $\left(\frac{3}{2}, \infty\right)$
- f is negative on the interval $\left(1, \frac{3}{2}\right)$.

5. By the quotient rule,

$$\begin{aligned} f'(x) &= \frac{(x-1)2 - (2x-3)1}{(x-1)^2} \\ &= \frac{1}{(x-1)^2}. \end{aligned}$$

The derivative f' is undefined at 1, and $f'(x) > 0$ for $x < 1$ and $x > 1$. Thus

- f is increasing on the intervals $(-\infty, 1)$ and $(1, \infty)$
- f has no stationary points.

6. The denominator of $f(x)$ is 0 when $x = 1$, so the line $x = 1$ is a vertical asymptote.

From step 4, $f(x)$ is positive as x tends to 1^-, and $f(x)$ is negative as x tends to 1^+.

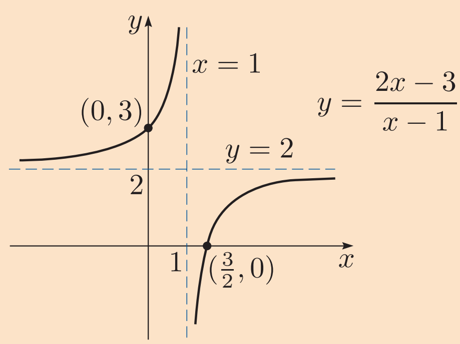
Thus, by the results of step 4,

$$f(x) \to \infty \text{ as } x \to 1^- \quad \text{and} \quad f(x) \to -\infty \text{ as } x \to 1^+.$$

To find the behaviour of f for large values of x, we compare the dominant term in the numerator, $2x$, with the dominant term in the denominator, x. Here the powers of x in these terms are equal, so there is a horizontal asymptote.

The dominant term of the numerator is $2x$, with coefficient 2, and the dominant term of the denominator is x, with coefficient 1. The power of x in the two dominant terms is the same, so the line $y = 2/1 = 2$ is a horizontal asymptote.

This information enables us to sketch the graph.



We could have rewritten the function in Worked Exercise A81 as

$$f(x) = \frac{2(x-1)-1}{x-1}$$
$$= 2 - \frac{1}{x-1}$$
$$= -\left(\frac{1}{x-1}\right) + 2,$$

and deduced that the graph of f can be obtained from the graph of $y = 1/x$ by a $(1, -1)$-scaling followed by a $(1, 2)$-translation. However, this translation and scaling are easier to deduce with hindsight, *after* sketching the graph, so unless a translation and/or a scaling of a standard graph are obvious, it is easiest to follow the strategy.

Exercise A151

Sketch the graph of the linear rational function

$$f(x) = \frac{x-3}{2-x}.$$

Next, we sketch the graph of a more complicated rational function.

Worked Exercise A82

Sketch the graph of the function

$$f(x) = \frac{x^2 - 5x + 4}{x^2 + 5x + 4}.$$

Solution

1. $$f(x) = \frac{x^2 - 5x + 4}{x^2 + 5x + 4} = \frac{(x-1)(x-4)}{(x+1)(x+4)}$$
   Thus the domain of f is $\mathbb{R} - \{-1, -4\}$.
2. The function is neither even nor odd, since the domain is not symmetric about 0.
3. We have $f(x) = 0$ when $(x-1)(x-4) = 0$, so the x-intercepts are 1 and 4. Also $f(0) = 4/4 = 1$, so the y-intercept is 1.
4. We construct a table of signs for f.

   To save space, we omit the first and last interval headings.

x		-4	$(-4,-1)$	-1	$(-1,1)$	1	$(1,4)$	4	
$x-1$	$-$	$-$	$-$	$-$	$-$	0	$+$	$+$	$+$
$x-4$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	0	$+$
$x+1$	$-$	$-$	$-$	0	$+$	$+$	$+$	$+$	$+$
$x+4$	$-$	0	$+$	$+$	$+$	$+$	$+$	$+$	$+$
$f(x)$	$+$	$*$	$-$	$*$	$+$	0	$-$	0	$+$

So

- f is positive on the intervals $(-\infty, -4)$, $(-1, 1)$ and $(4, \infty)$
- f is negative on the intervals $(-4, -1)$ and $(1, 4)$.

5. Use the quotient rule to differentiate f. This is simpler if we rearrange the expression for f first, but it is not essential to spot this.

We have

$$f(x) = \frac{x^2 - 5x + 4}{x^2 + 5x + 4} = 1 - \frac{10x}{x^2 + 5x + 4}.$$

Thus, by the quotient rule,

$$\begin{aligned} f'(x) &= \frac{(x^2 + 5x + 4)(-10) - (-10x)(2x + 5)}{(x^2 + 5x + 4)^2} \\ &= \frac{10(x^2 - 4)}{(x^2 + 5x + 4)^2} \\ &= \frac{10(x - 2)(x + 2)}{(x + 1)^2(x + 4)^2}. \end{aligned}$$

We construct a table of signs for f'.

x		-4	$(-4, -2)$	-2	$(-2, -1)$	-1	$(-1, 2)$	2	
$10(x - 2)$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	0	$+$
$x + 2$	$-$	$-$	$-$	0	$+$	$+$	$+$	$+$	$+$
$(x + 1)^2$	$+$	$+$	$+$	$+$	$+$	0	$+$	$+$	$+$
$(x + 4)^2$	$+$	0	$+$	$+$	$+$	$+$	$+$	$+$	$+$
$f'(x)$	$+$	$*$	$+$	0	$-$	$*$	$-$	0	$+$

So, using this table and the First Derivative Test, we deduce that

- f is increasing on the intervals $(-\infty, -4)$, $(-4, -2)$ and $(2, \infty)$
- f is decreasing on the intervals $(-2, -1)$ and $(-1, 2)$
- f has stationary points at -2 and 2
- there is a local maximum at $x = -2$ with $f(-2) = -9$
- there is a local minimum at $x = 2$ with $f(2) = -\frac{1}{9}$.

6. The denominator is 0 when $x = -4$ or $x = -1$, so the lines $x = -4$ and $x = -1$ are vertical asymptotes.

Thus, by the results of step 4,

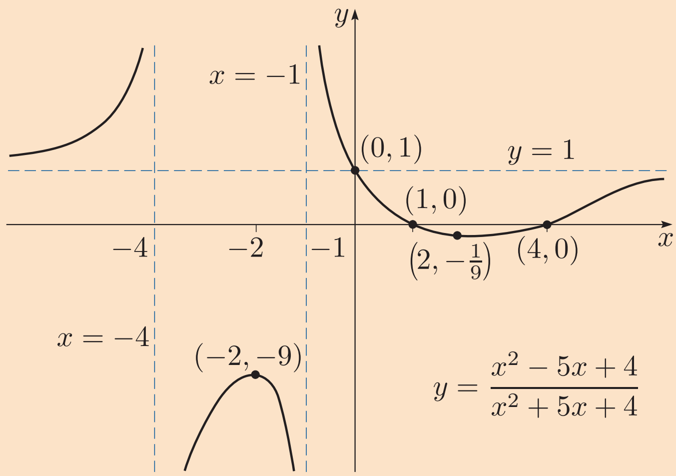
$$f(x) \to \infty \text{ as } x \to -4^- \quad \text{and} \quad f(x) \to -\infty \text{ as } x \to -4^+;$$
$$f(x) \to -\infty \text{ as } x \to -1^- \quad \text{and} \quad f(x) \to \infty \text{ as } x \to -1^+.$$

To find the behaviour of f for large values of x, we compare the dominant term of the numerator with the dominant term of the denominator. Here the powers of x in these terms are equal, so there is a horizontal asymptote.

The dominant term in both the numerator and the denominator is x^2. Thus the power of x is the same in each case. The ratio of the coefficients of the dominant terms is 1. Therefore the line $y = 1$ is a horizontal asymptote.

This information enables us to sketch the graph.

Here the difference in the y-coordinates of the stationary points makes it hard to draw all the graph's features clearly, so we exaggerate the vertical scale at the local minimum.



Exercise A152

Sketch the graph of the rational function

$$f(x) = \frac{1}{x(x+1)^2}.$$

The same ideas can be used to sketch the graph of a function that is not rational or polynomial, as shown by the application of Strategy A3 in the next worked exercise.

Worked Exercise A83

Sketch the graph of $f(x) = \dfrac{1}{\sqrt{1+x^2}}$

Solution

1. The domain of f is $\mathbb{R}$.
2. f is even, since, for all x in $\mathbb{R}$,
$$f(-x) = \frac{1}{\sqrt{1+(-x)^2}} = \frac{1}{\sqrt{1+x^2}} = f(x).$$
3. The equation $f(x) = 0$ has no solution, so there are no x-intercepts.

   The y-intercept is $f(0) = 1$.
4. There is no need for a table of signs.

   f is positive on $\mathbb{R}$.
5. Use the chain rule to differentiate $f(x) = (1+x^2)^{-\frac{1}{2}}$.

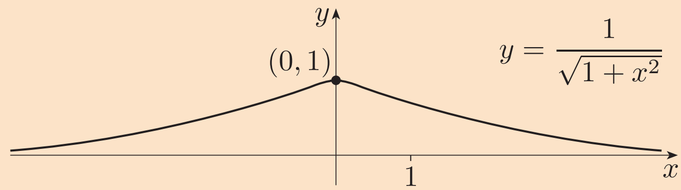
   By the chain rule,
$$\begin{aligned} f'(x) &= -\frac{1}{2}(1+x^2)^{-3/2}(2x) \\ &= -\frac{x}{(1+x^2)^{3/2}}, \end{aligned}$$
   so the denominator of f' is always positive, and therefore
$$\begin{aligned} &f'(x) = 0 \quad \text{when } x = 0 \\ &f'(x) < 0 \quad \text{when } x > 0 \\ &f'(x) > 0 \quad \text{when } x < 0. \end{aligned}$$
   We deduce that,
   - f is decreasing on the interval $(0, \infty)$
   - f is increasing on the interval $(-\infty, 0)$
   - f has a stationary point at $x = 0$.

   By the First Derivative Test, we deduce that there is a local maximum at $x = 0$. We have $f(0) = 1$.
6. This is not a rational function, but similar arguments work here to find a horizontal asymptote. As x become large and positive, the 1 in the denominator $\sqrt{1+x^2}$ becomes insignificant compared to the value of x^2, so the function f behaves in a similar way to $g(x) = 1/x$.

   As x becomes large and positive the function behaves in a similar way to the more familiar function $g(x) = 1/x$. Therefore the line $y = 0$ is a horizontal asymptote.

   The function is even so we have
$$f(x) \to 0 \quad \text{as } x \to \pm\infty.$$

This information enables us to sketch the graph.



In this section we have used the First Derivative Test to determine whether a given stationary point is a local maximum, a local minimum or neither. You may have met the following alternative test for a local maximum or local minimum.

Second Derivative Test

Suppose that a is a stationary point of a differentiable function f, so that $f'(a) = 0$.

- If $f''(a) < 0$, then f has a local maximum at a.
- If $f''(a) > 0$, then f has a local minimum at a.

This test can be very efficient as a means of classifying stationary points. However, for some functions it is too complicated to find the second derivative. Moreover, if $f''(a) = 0$, then the Second Derivative Test gives no result: the stationary point may be a local maximum, a local minimum, or neither. This is why Strategy A3 uses the First Derivative Test. However, it is fine for you to use the Second Derivative Test when it is convenient.

3 New graphs from old

In this section you will extend your graph sketching capabilities to include the graphs of combinations of functions, including sums and products of two functions, composite functions and hybrid functions.

3.1 Further graph-sketching techniques

We start by looking at some techniques for sketching the graph of a combination of two functions, one of which is a trigonometric function.

To do this, we follow the steps of Strategy A3 as far as possible, but in some cases we find that part or all of some steps are not necessary, or too tricky to apply. We can also exploit known features of the trigonometric functions, such as the fact that the values of $\sin x$ and $\cos x$ oscillate (with period 2π) between the values 1 and -1. Because of this oscillation, it is often convenient to use other simple graphs as *construction lines* for the graph we are sketching. So, for this subsection, we add another step to Strategy A3 as follows.

Strategy A4 Extended graph-sketching strategy

To sketch the graph of a function f, determine the following features of f (where possible), and show these features in your sketch.

1. The domain of f.
2. Whether f is even, odd or periodic (or none of these).
3. The x-intercepts and the y-intercept of f, if any.
4. The intervals on which f is positive or negative.
5. The intervals on which f is increasing or decreasing, the nature of any stationary points, and the value of f at each of these points.
6. The asymptotic behaviour of f.
7. Any appropriate construction lines, and the points where f meets these lines.

The following worked exercise illustrates Strategy A4.

Worked Exercise A84

Sketch the graph of the function

$$f(x) = x \sin x.$$

Solution

We use Strategy A4 as far as possible.

1. The function f has domain $\mathbb{R}$.
2. The function f is even since, for all x in $\mathbb{R}$,

   $$f(-x) = -x \sin(-x) = x \sin x = f(x).$$

   It is therefore sufficient initially to consider the features of the graph of f for $x \geq 0$ and then to reflect the graph we obtain in the y-axis.

Although this function involves a trigonometric function, it seems unlikely to be periodic because of the factor of x, so we omit this test.

3. We have $f(x) = 0$ when $x = 0$ or when $\sin x = 0$.

   For $x \geq 0$, $\sin x = 0$ when $x = 0, \pi, 2\pi, \ldots$.

   For $x \geq 0$, the x-intercepts are $0, \pi, 2\pi, \ldots$.

   The y-intercept is 0 since $f(0) = 0$.

4. The intervals on which f is positive or negative (for $x > 0$) alternate between the x-intercepts in the same way as for the sine function.

   For $x > 0$,

   - f is positive on $(0, \pi), (2\pi, 3\pi), \ldots$
   - f is negative on $(\pi, 2\pi), (3\pi, 4\pi), \ldots$.

5. Differentiating gives $f'(x) = \sin x + x \cos x$, but $f'(x) = 0$ is not easy to solve. We can obtain enough information to sketch the graph from other steps.

   $f'(x) = \sin x + x \cos x$, so we omit solving $f'(x) = 0$, as it is not easy.

6. The function f has no asymptotes as it is defined for all values of x and does not tend to a limit as x tends to $\pm\infty$.

   The function f has no asymptotes.

7. Here we use what we know about the sine function.

   Since $-1 \leq \sin x \leq 1$, for all real numbers x, we have

   $$-x \leq x \sin x \leq x, \quad \text{for } x > 0.$$

   That is,

   $$-x \leq f(x) \leq x, \quad \text{for } x > 0,$$

   so, for $x > 0$, the graph of f lies between the lines $y = x$ and $y = -x$. These are the construction lines for this function.

   The function f, for $x > 0$, has the following features:

   $$f(x) = x \text{ when } \sin x = 1$$

   $$f(x) = -x \text{ when } \sin x = -1.$$

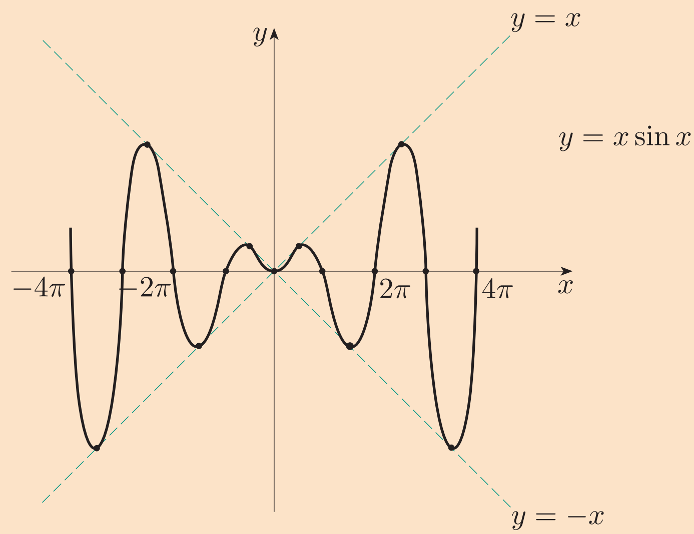
   $\sin x = 1$ when $x = \pi/2, 5\pi/2, \ldots$, and $\sin x = -1$ when $x = 3\pi/2, 7\pi/2, \ldots$.

   For $x > 0$, the graph of the function f

   - meets the construction line $y = x$ when $x = \pi/2, 5\pi/2, \ldots$
   - meets the construction line $y = -x$ when $x = 3\pi/2, 7\pi/2, \ldots$.

This information enables us to sketch the graph.

We start by drawing the construction lines $y = x$ and $y = -x$. Then we draw dots to indicate the points where the graph of f meets these construction lines and where it crosses the x-axis. We complete the sketch by drawing a smooth curve through these points and then reflecting the graph in the y-axis.



The sketch produced in the worked exercise above does not give the precise positions of the local maxima and minima of the graph of the function: it is not a precise drawing, but a sketch indicating the general behaviour and most of the important features. It can be shown that the dots on $y = x$ and $y = -x$ are not actually the local maxima and minima, as the more accurate enlargement in Figure 29 illustrates.

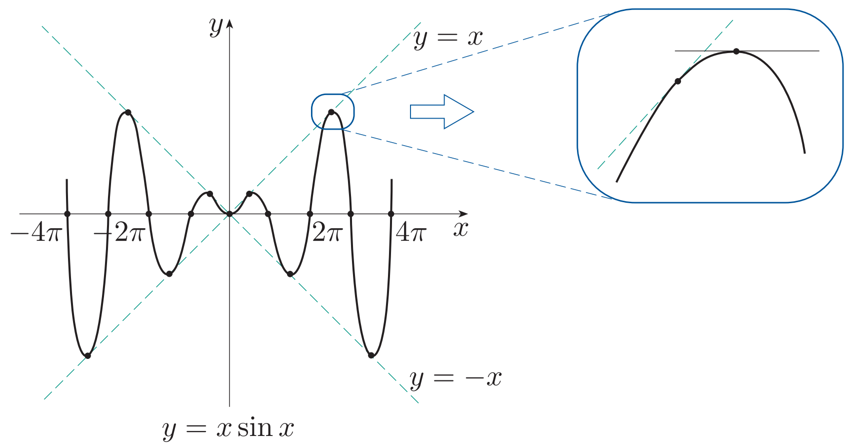


Figure 29 Enlargement of the graph of the function $f(x) = x \sin x$

Exercise A153

Sketch the graph of the function $f(x) = x\cos x$.

Exercise A154

Sketch the graph of the function $f(x) = x + \sin x$.

So far in this section we have considered combinations of functions involving sums and products. We now briefly consider the graphs of some composite functions.

Recall that a **composite function** is a function, such as $f(x) = \sin(1/x)$, that can be obtained by applying first one function (here, $x \longmapsto 1/x$) and then another function (here, $x \longmapsto \sin x$).

We can use the extended graph-sketching strategy (Strategy A4) to sketch the graphs of some composite functions, including $f(x) = \sin(1/x)$. However, we begin by noting that there are some composite functions where the properties of one of the functions allows you to 'spot' the behaviour of the composite function without needing to work through the strategy. The next exercise is one such case.

Exercise A155

Sketch the graph of the composite function

$$f(x) = |\sin x|.$$

Note that in Exercise A155 it would not have been possible to use calculus to find the local maxima and minima because the function $f(x) = |\sin x|$ is not a differentiable function (its graph has sharp corners).

The remainder of this subsection is useful preparation for the analysis units of this module, but you will not be assessed on it at this stage. If you are short of time now, you could read the rest of this subsection quickly and revisit it later.

If a composite function involves a trigonometric function, then we can exploit known features of the trigonometric function in sketching its graph, just as we did in some of the earlier worked exercises.

Consider the function

$$f(x) = \sin\frac{1}{x}.$$

We can apply the strategy, and the first few steps follow in much the same way as in Worked Exercise A84: the domain of f is $\mathbb{R} - \{0\}$, the function is odd and there is no y-intercept since f is not defined when $x = 0$.

The x-intercepts are the values of x for which $f(x) = 0$; that is, when $\sin(1/x) = 0$. For $x > 0$, this is when $1/x = \pi, 2\pi, 3\pi, \ldots$, so the x-intercepts are

$$\frac{1}{\pi}, \frac{1}{2\pi}, \frac{1}{3\pi}, \ldots.$$

Thus a big difference between the graph of this function and the one in Worked Exercise A84 is that here the x-intercepts, or zeros, become ever closer together as x approaches 0 from the right. It follows that, as x approaches 0 from the right, the intervals on which f is positive or negative become progressively smaller, and the local maxima and minima become progressively closer together: the oscillations of the graph bunch closer and closer together as x approaches 0 from the right.

For $x > 0$, it can be shown that f

- is positive on $\left(\frac{1}{\pi}, \infty\right)$, and on $\left(\frac{1}{3\pi}, \frac{1}{2\pi}\right), \left(\frac{1}{5\pi}, \frac{1}{4\pi}\right), \ldots,$
- is negative on $\left(\frac{1}{2\pi}, \frac{1}{\pi}\right), \left(\frac{1}{4\pi}, \frac{1}{3\pi}\right), \ldots,$
- has maxima when $x = \frac{2}{\pi}, \frac{2}{5\pi}, \frac{2}{9\pi}, \ldots$ with $f(x) = 1$,
- has minima when $x = \frac{2}{3\pi}, \frac{2}{7\pi}, \frac{2}{11\pi}, \ldots$ with $f(x) = -1$,
- tends to 0, as $x \to \infty$.

Therefore the lines $y = \pm 1$ are construction lines, and $y = 0$ is a horizontal asymptote.

A sketch of the graph of $y = \sin(1/x)$ is shown in Figure 30. Note that the function is not defined at the origin, and it is not possible to sketch the graph in the region close to the origin where the oscillations become closer and closer together.

You will meet this function again in the analysis units in Book D *Analysis 1* of this module.

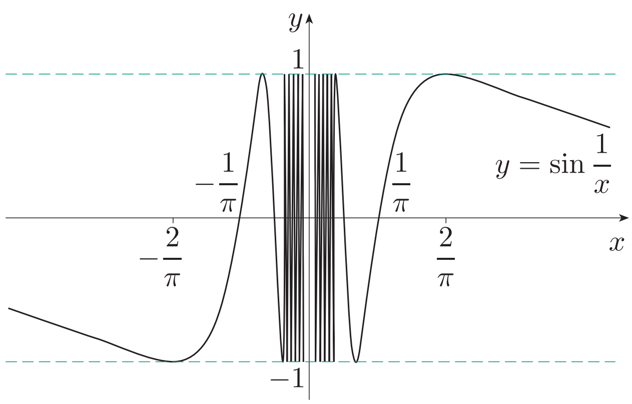


Figure 30 A sketch of the graph of the function $f(x) = \sin\frac{1}{x}$

We finish this subsection by looking at another function which is not defined when $x = 0$. This function is a quotient of two functions, one of which is a trigonometric function:

$$f(x) = \frac{\sin x}{x}.$$

Again, we can apply the strategy, and the steps follow in much the same way as in Worked Exercise A84: the domain of f is $\mathbb{R} - \{0\}$, the function is even and there is no y-intercept, since f is not defined at $x = 0$.

The x-intercepts are the values of x for which $(\sin x)/x = 0$; that is, when $x = \pi, 2\pi, 3\pi, \ldots$. The intervals on which f is positive or negative alternate between these x-intercepts in the same way as for the sine function.

Now, $-1 \leq \sin x \leq 1$, so

$$-\frac{1}{x} \leq \frac{\sin x}{x} \leq \frac{1}{x}.$$

Therefore, for $x > 0$, the curves $y = 1/x$ and $y = -1/x$ are construction lines.

This is almost enough information to sketch the graph of f, but what happens as x approaches 0? It turns out that

$$\frac{\sin x}{x} \to 1 \text{ as } x \to 0,$$

though you cannot deduce this from what you know so far. You will see a proof of this result in Book F.

A sketch of the graph of $y = (\sin x)/x$ is shown in Figure 31.

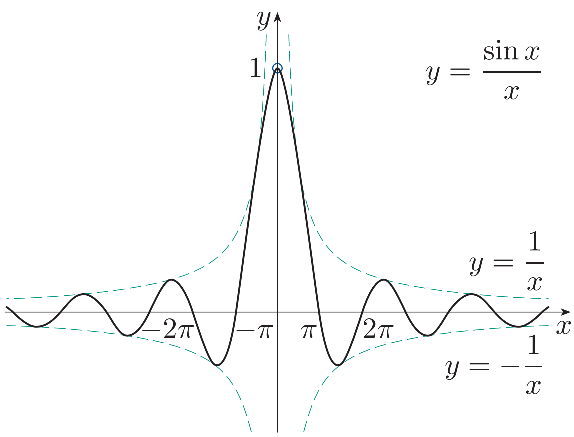


Figure 31 A sketch of the graph of the function $f(x) = (\sin x)/x$

The graph of this function has a 'hole' when $x = 0$, and it seems natural to fill this hole by defining $f(0) = 1$. In this way, we can extend the domain of this function to include 0:

$$g(x) = \begin{cases} \dfrac{\sin x}{x}, & x \neq 0, \\ 1, & x = 0. \end{cases}$$

This is an example of a *hybrid function*; hybrid functions will be defined in the next subsection. You will meet this function g again in Book F, where you will see that, with this definition, the function is *continuous* at 0.

However, for the function $f(x) = \sin(1/x)$ sketched in Figure 30, we cannot 'fill in the hole' at $x = 0$ by defining an appropriate hybrid function: whatever value we assign to $f(0)$, we cannot extend the domain of the function to the whole of $\mathbb{R}$ so that it is continuous at 0. You will also see this in Book D.

3.2 Hybrid functions

You have seen that the rule of a function is one of its main components, which may suggest that a function always has a single formula associated with it, but this is not the case. Some functions of the greatest practical importance are **hybrid functions** that have rules which are defined by different formulas on different parts of their domains.

To specify a hybrid function, we need to state which rule applies on which part of the domain, and we use a curly bracket to list the different cases. For example, consider the function

$$f(x) = \begin{cases} 1, & 1 < x \leq 2, \\ 0, & x \leq 1 \text{ and } x > 2. \end{cases}$$

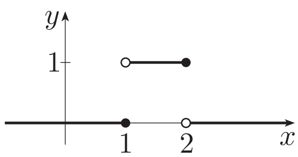


Figure 32 The graph of the hybrid function f

The function f has domain $\mathbb{R}$, since f is defined for each x in $\mathbb{R}$ and for each such x, there is a unique value of f. It takes the value 1 on the interval $(1, 2]$, and the value 0 elsewhere, as illustrated in Figure 32.

Worked Exercise A85

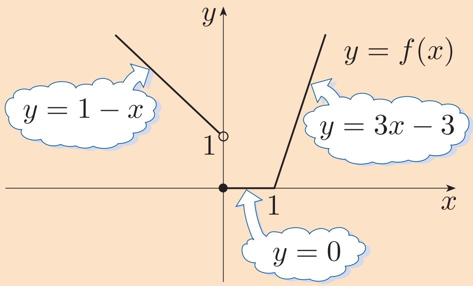
Sketch the graph of the function

$$f(x) = \begin{cases} 1-x, & x<0, \\ 0, & 0 \le x \le 1, \\ 3x-3, & x>1. \end{cases}$$

Solution

The function f has domain $\mathbb{R}$.

We use our knowledge of the graphs $y = 1-x$, $y=0$, and $y = 3x-3$, to build up the parts of this hybrid function. This enables us to construct the following sketch.



You will recognise that the graph of the function in Worked Exercise A85 is not smooth: it has a 'jump' at $x=0$ and a 'corner' at $x=1$. The meanings of these features will be made precise in Books D and F.

Exercise A156

Sketch the graph of each of the following hybrid functions.

(a) $f(x) = \begin{cases} x^2, & x \le 1 \\ \sqrt{x}, & x>1 \end{cases}$ (b) $f(x) = \begin{cases} e^x, & x<0 \\ |x-1|, & 0 \le x \le 2 \\ x-2, & x>2 \end{cases}$

(c) $f(x) = \begin{cases} x^2, & x<0 \\ \sin x, & x \ge 0 \end{cases}$

4 Hyperbolic functions

In this section you will revise *hyperbolic functions* and explore their properties.

4.1 Properties of hyperbolic functions

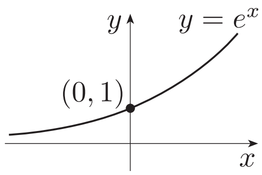


Figure 33 The graph of the exponential function

In Subsection 1.2 you met the graph of the exponential function $f(x) = e^x$, often referred to as exp, which is shown in Figure 33. The function exp has the following properties which will be explained and discussed in greater detail in Books D and F:

- the domain of exp is $\mathbb{R}$
- exp is not even, odd or periodic
- $e^x > 0$ for all x in $\mathbb{R}$, so exp is positive on $\mathbb{R}$
- exp is its own derivative – that is, if $f(x) = e^x$, then $f'(x) = e^x$
- since $e^x > 0$ for all x in $\mathbb{R}$, exp is increasing on $\mathbb{R}$
- $e^0 = 1$, $e^x > 1$ for all $x > 0$ and $e^x < 1$ for all $x < 0$
- $e^{x+y} = e^x e^y$ for all x, y in $\mathbb{R}$
- $e^x \to \infty$ as $x \to \infty$ and $e^x \to 0$ as $x \to -\infty$
- if n is any positive integer, then $e^x/x^n \to \infty$ as $x \to \infty$.

We sometimes express this final property by saying that e^x *grows faster than any polynomial when x is large.*

The following exercise gives you some practice in manipulating exponential terms.

Exercise A157

Simplify each of the following expressions so that it involves no products or quotients.

(a) $e^x(e^x + e^{-x})$ (b) $(e^{2x} - e^{-2x})/e^x$ (c) $(e^{5x} + e^{-5x})(e^{5x} - e^{-5x})$

Certain combinations of e^x and e^{-x} appear so frequently in mathematics that it is useful to introduce functions that express these combinations more concisely. The functions that we need are the **hyperbolic functions** cosh, sinh and tanh, all of which have domain $\mathbb{R}$:

- cosh is the **hyperbolic cosine function**, with rule

$$\cosh x = \frac{1}{2}\left(e^x + e^{-x}\right)$$

- sinh is the **hyperbolic sine function**, with rule

$$\sinh x = \frac{1}{2}\left(e^x - e^{-x}\right)$$

- tanh is the **hyperbolic tangent function**, with rule

$$\tanh x = \frac{\sinh x}{\cosh x}.$$

It is usual to pronounce 'cosh' as it is spelled, 'sinh' as 'sinsh' or 'shine', and 'tanh' as 'tansh' or 'than' (as in 'thank').

The name 'hyperbolic' originates from the use of these functions as parametric forms for a *hyperbola*, a type of *conic*. You will meet conics and their parametric forms in Section 5.

The first systematic development of hyperbolic functions was by Johann Heinrich Lambert (1728–1777) in the mid-eighteenth century, although it is now known that there is a link between hyperbolic functions and the formulas used by the Flemish cartographer Gerardus Mercator (1512–1594) in the construction of his map projection of 1569. In the nineteenth century, the widespread use of electricity led to an increased interest in hyperbolic functions due to their application in the transmission of electrical power.

Gerardus Mercator

At first sight, the hyperbolic functions seem unrelated to the trigonometric functions, but in fact there is a very strong connection between them, which becomes apparent when we view the hyperbolic functions as *complex* functions, that is, functions whose domain is $\mathbb{C}$. To see that such a connection exists, recall Euler's Formula,

$$e^{ix} = \cos x + i\sin x, \quad \text{for } x \in \mathbb{R},$$

from Unit A2 *Number systems*. It follows that

$$\begin{aligned} e^{-ix} &= \cos(-x) + i\sin(-x) \\ &= \cos x - i\sin x, \end{aligned}$$

and therefore

$$\cos x = \frac{1}{2}\left(e^{ix} + e^{-ix}\right) \quad \text{and} \quad \sin x = \frac{1}{2i}\left(e^{ix} - e^{-ix}\right).$$

If you compare these expressions with the definitions of cosh and sinh, you will see that

$$\cosh(ix) = \cos x \quad \text{and} \quad \sinh(ix) = i\sin x.$$

You will learn more about complex functions if you take your study of pure mathematics further. In this unit, you will only study the hyperbolic functions as *real* functions. You will see that in some ways they behave like the corresponding trigonometric functions, but in other ways they are quite different.

The next two exercises demonstrate some similarities between the hyperbolic functions cosh and sinh and the trigonometric functions cos and sin. Note that $\cosh^2 x$ and $\sinh^2 x$ are abbreviations for $(\cosh x)^2$ and $(\sinh x)^2$, respectively.

Exercise A158

Using the definitions above, prove the following.

(a) $\cosh^2 x - \sinh^2 x = 1$

(b) $\cosh(x + y) = \cosh x \cosh y + \sinh x \sinh y$

(c) $\sinh(x + y) = \sinh x \cosh y + \cosh x \sinh y$

Hint: In parts (b) and (c), start from the right-hand side.

Exercise A159

Find the derivatives of the functions $\cosh x$ and $\sinh x$, and compare your answers with the derivatives of $\cos x$ and $\sin x$.

As you might expect, we can also define three other hyperbolic functions:

$$\operatorname{sech} x = \frac{1}{\cosh x}, \quad \text{just as } \sec x = \frac{1}{\cos x},$$

$$\operatorname{cosech} x = \frac{1}{\sinh x}, \quad \text{just as } \operatorname{cosec} x = \frac{1}{\sin x},$$

$$\coth x = \frac{1}{\tanh x}, \quad \text{just as } \cot x = \frac{1}{\tan x}.$$

These functions are the **hyperbolic secant function**, the **hyperbolic cosecant function**, and the **hyperbolic cotangent function**, respectively. It is usual to pronounce 'sech' as 'sesh' or 'sheck', 'cosech' as 'co-sesh' or 'co-sheck', and 'coth' to rhyme with 'moth'.

In Exercise A158 you met some identities involving cosh and sinh that are very similar to identities involving cos and sin. In fact, for every identity satisfied by trigonometric functions, there is a corresponding identity involving hyperbolic functions. A table comparing the most useful trigonometric and hyperbolic identities is included in the module Handbook.

4.2 Graphs of hyperbolic functions

We now turn our attention to sketching the graphs of the hyperbolic functions. You will see that they bear little or no resemblance to the graphs of the corresponding trigonometric functions.

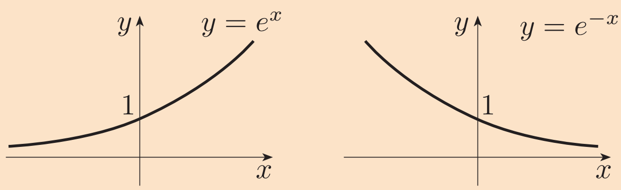
Worked Exercise A86

Sketch the graph of the function

$$f(x) = \cosh x.$$

Solution

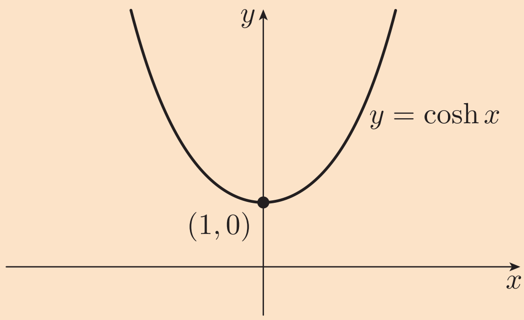
Since $\cosh x = \frac{1}{2}(e^x + e^{-x})$, we have to 'take the average' of the graphs of $y = e^x$ and $y = e^{-x}$: for each value of x, the required value is halfway between the values for these graphs. A sketch helps here.



We use Strategy A3.

1. $f(x) = \cosh x$ has domain $\mathbb{R}$.
2. f is even, since, for all x in $\mathbb{R}$,
$$\begin{aligned} f(-x) = \cosh(-x) &= \tfrac{1}{2}\left(e^{-x} + e^{-(-x)}\right) \\ &= \tfrac{1}{2}\left(e^{x} + e^{-x}\right) = \cosh x = f(x). \end{aligned}$$
It is therefore sufficient to consider the features of the graph of f for $x \geq 0$, and then to reflect the graph in the y-axis.
3. To find any x-intercepts of f we have to solve the equation
$$\tfrac{1}{2}\left(e^x + e^{-x}\right) = 0.$$
However, e^x and e^{-x} are positive for all x in $\mathbb{R}$, so $\cosh x$ is positive for all x in $\mathbb{R}$.
The entire graph lies above the x-axis.
Thus f has no x-intercepts.
Also, $f(0) = \frac{1}{2}\left(e^0 + e^{-0}\right) = \frac{1}{2}(1+1) = 1$, so the y-intercept is 1.
4. As shown in step 3, $\cosh x$ is positive for all x in $\mathbb{R}$.
5. $f'(x) = \sinh x = \frac{1}{2}(e^x - e^{-x})$.
The graphs of $y = e^x$ and $y = e^{-x}$ show that $e^x > e^{-x}$ for $x > 0$, so $\sinh x > 0$ for $x > 0$.
So $f'(x)$ is positive when $x > 0$ and zero when $x = 0$, and
   - f is increasing on the interval $(0, \infty)$
   - f has a local minimum at 0, with value $\cosh(0) = 1$.
6. Since $e^x \to \infty$ as $x \to \infty$ and $e^{-x} \to 0$ as $x \to \infty$,
$$\cosh x \to \infty \quad \text{as } x \to \infty.$$

This information enables us to sketch the graph.



So the graph of the cosh function bears little resemblance to that of the cosine function; for example,

$$\cosh x \geq 1, \quad \text{for all } x \text{ in } \mathbb{R},$$

whereas

$$-1 \leq \cos x \leq 1, \quad \text{for all } x \text{ in } \mathbb{R}.$$

Moreover, unlike the cosh function, the cosine function is periodic with period 2π, so its graph looks the same on successive intervals of length 2π.

By working through the next exercise, you will discover that there is also little similarity between the graphs of the sinh function and the sine function.

Exercise A160

Sketch the graph of the function

$$f(x) = \sinh x.$$

Using the properties of the functions cosh and sinh, we can now sketch the graphs of their reciprocals, sech and cosech. Graphs of all the hyperbolic functions are given in the module Handbook for reference.

Worked Exercise A87

Sketch the graph of the function

$$f(x) = \operatorname{sech} x = \frac{1}{\cosh x}.$$

Solution

We use Strategy A3.

We use what we know about $\cosh x$.

1. f has domain $\mathbb{R}$, since $\cosh x$ is never 0.
2. f is an even function, since $\cosh x$ is an even function. It is therefore sufficient to consider the features of the graph of f for $x \geq 0$, and then to reflect the graph we obtain in the y-axis.
3. We know that $\cosh x \geq 1$ for all x in $\mathbb{R}$, so, for all x in $\mathbb{R}$,

   $$0 < \operatorname{sech} x \leq 1.$$

   So f has no x-intercepts.

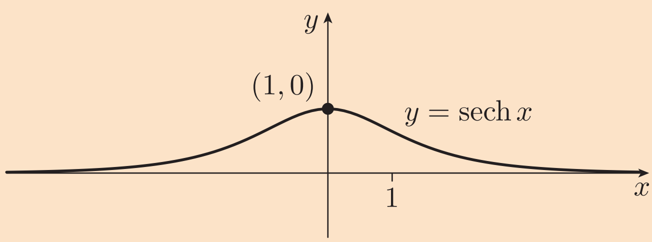
   $$f(0) = \operatorname{sech} 0 = \frac{1}{\cosh 0} = \frac{1}{1} = 1,$$

   so the y-intercept is 1.
4. As shown in step 3, f is positive for all $x \in \mathbb{R}$.
5. Since $\cosh x$ is increasing on $(0, \infty)$ and has a local minimum at 0,
   - $\operatorname{sech} x$ is decreasing on $(0, \infty)$
   - $\operatorname{sech} x$ has a local maximum at 0 with value $\operatorname{sech}(0) = 1$.
6. Since $\cosh x \to \infty$ as $x \to \pm\infty$, we have

   $$\operatorname{sech} x \to 0 \text{ as } x \to \pm\infty.$$

   So $y = 0$ is a horizontal asymptote.

This information enables us to produce the following sketch.



Exercise A161

Sketch the graph of the function

$$f(x) = \operatorname{cosech} x.$$

5 Conics

In this section you will revise *conics*: circles, ellipses, parabolas and hyperbolas.

5.1 Conic sections

In your previous studies you will have met three different ways to define a *conic*: by slicing a double cone with a plane; geometrically, using the focus-directrix definition, and algebraically, using an equation. You will review all three ways in this section. The three definitions are equivalent, but the proof of this is not given here.

A **conic section**, or **conic**, is a curve obtained by slicing a double cone with a plane, as illustrated in Figures 34 to 37. The type of conic obtained depends on the orientation of the slicing plane, as indicated in the figures.

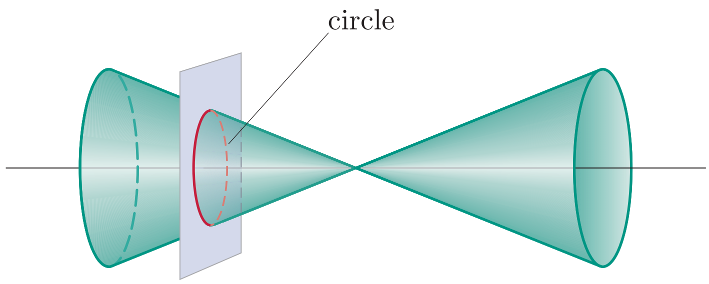


Figure 34 Slicing a double cone to obtain a circle (plane perpendicular to axis)

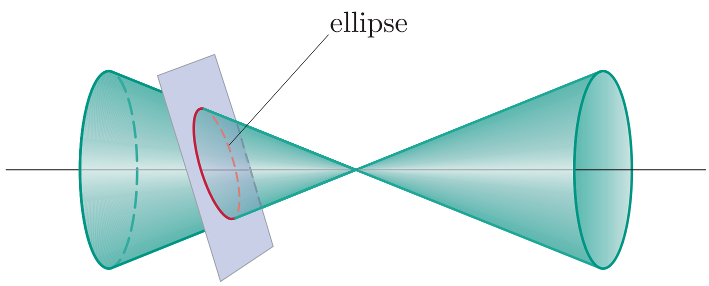


Figure 35 Slicing a double cone to obtain an ellipse (plane tilted slightly from the perpendicular)

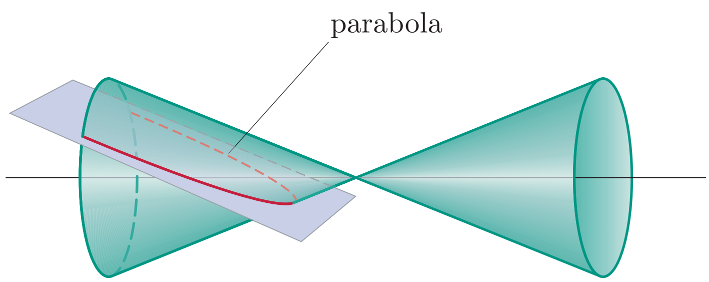


Figure 36 Slicing a double cone to obtain a parabola (plane parallel to side of cone)

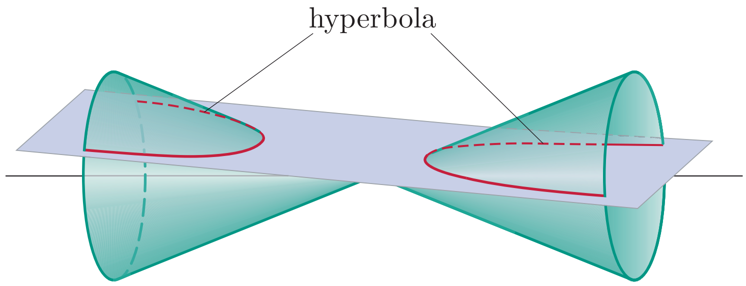


Figure 37 Slicing a double cone to obtain a hyperbola (plane tilted further)

A **degenerate conic section**, or **degenerate conic**, is obtained when the slicing plane passes through the apex of the double cone. It may be a single point, a straight line or two intersecting straight lines, as illustrated in Figure 38.

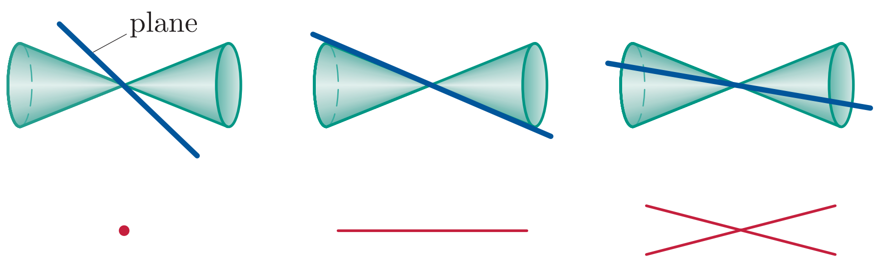


Figure 38 Degenerate conics obtained by slicing a double cone

A **non-degenerate conic section**, or **non-degenerate conic**, is a conic that is not degenerate. It may be a circle, an ellipse, a parabola or a hyperbola; sometimes a circle is considered to be a special type of ellipse.

A **circle** can be defined geometrically as the set of points P such that the distance of P from a fixed point, the **centre**, is constant, as illustrated in Figure 39.

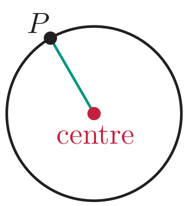


Figure 39 A circle

An ellipse, a parabola, and a hyperbola can also all be defined geometrically as the set of points whose distance from a fixed point and a fixed line are related. (In this unit, when we refer to the distance between a point and a line, we always mean the *shortest* such distance.) It can be shown that the set of points P such that the distance of P from a fixed point is a constant multiple, e, of the distance of P from a fixed line is

- an **ellipse** if $0 < e < 1$
- a **parabola** if $e = 1$
- a **hyperbola** if $e > 1$.

The fixed point is called the **focus** of the conic, the fixed line is called its **directrix**, and the constant multiple e is called its **eccentricity**. These focus–directrix properties are illustrated in Figure 40. (It seems natural to use the letter e for eccentricity. Of course, this is quite unrelated to the use of e as the symbol for the irrational number $2.718\ldots$, mentioned in Subsection 1.2).

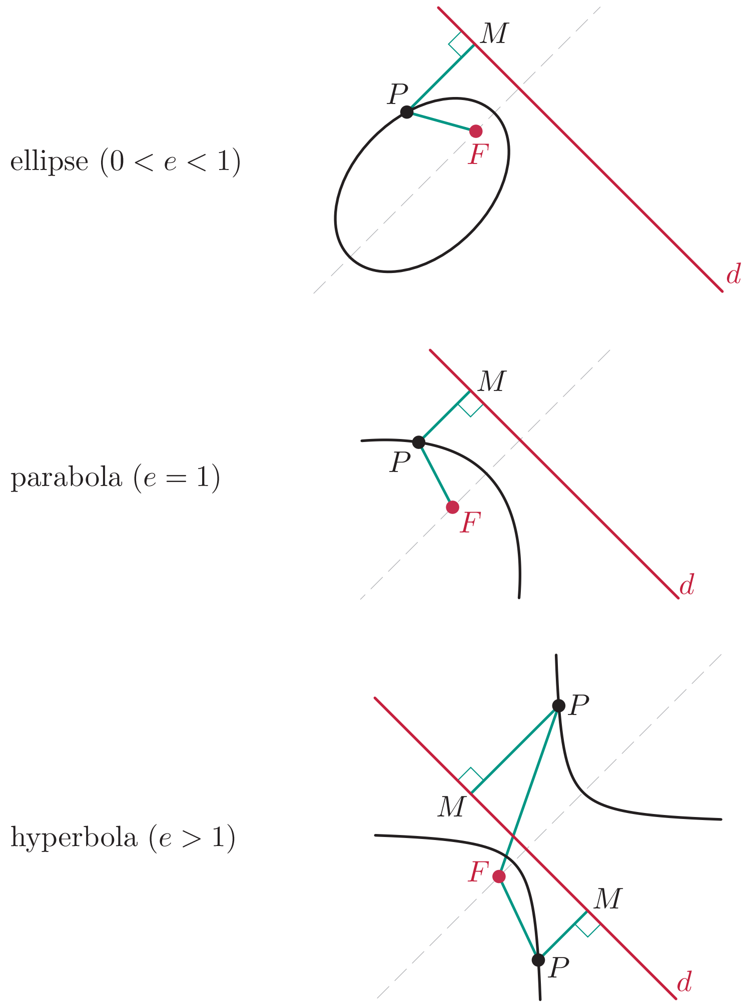


Figure 40 An ellipse, parabola and hyperbola obtained from a focus F and directrix d, with eccentricity $e = PF/PM$

The circle has no focus–directrix property, though some texts consider the focus to be the centre of the circle and the directrix to be 'at infinity', so that the circle is obtained when $e = 0$.

The ellipse, the parabola and the hyperbola were given their names by the Greek geometer Apollonius (c.262–c.190 BCE) in his *Conics*, a work of eight books completed in about 200 BCE which completely reformed the ancient study of conic sections. *Conics* was translated by the astronomer Edmund Halley (1656–1742) and published in 1710, see Figure 41.

Figure 41 Frontispiece of Apollonius' *Conics*

A (non-degenerate) conic is said to be in **standard position** if it is positioned in the plane as follows:

- For a circle: its centre is at the origin.
- For an ellipse: its axes of symmetry are the x- and y-axes, and its largest width is along the x-axis.
- For a parabola: its axis of symmetry is the x-axis, it passes through the origin and its other points lie to the right of the origin.
- For a hyperbola: its axes of symmetry are the x- and y-axes, and it crosses the x-axis.

An ellipse, a parabola and a hyperbola all in standard position are illustrated in Figure 42.

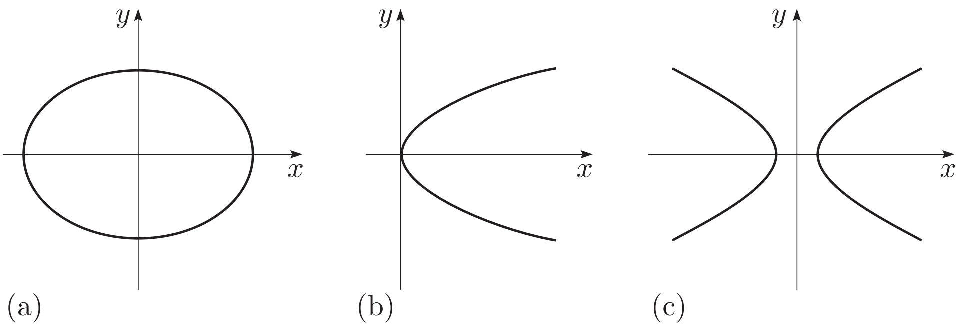


Figure 42 Conics in standard position: (a) ellipse (b) parabola and (c) hyperbola

Any conic, lying anywhere in the plane, can be rotated and translated so that it is in standard position. The equation of a conic in standard position can be always be expressed in a straightforward and easily recognisable form. The equations of conics in other positions are more complicated; you will meet the general equation of a conic in Subsection 5.3.

5.2 Conics in standard position

In this subsection you will look individually at the circle, the parabola, the ellipse and the hyperbola in standard position and consider their focus–directrix definitions and equations.

Circle

In Unit A1 you saw that the equation of a circle of radius a with its centre at the origin is

$$x^2 + y^2 = a^2.$$

Such a circle is in standard position.

Parabola ($e = 1$)

A parabola is the set of points P in the plane whose distances from a fixed point F are equal to their distances from a fixed line d.

A parabola is in standard position if

- the focus F lies on the x-axis, with coordinates $(a, 0)$, where $a > 0$
- the directrix d is the line with equation $x = -a$.

The features of a parabola in standard position are shown in Figure 43.

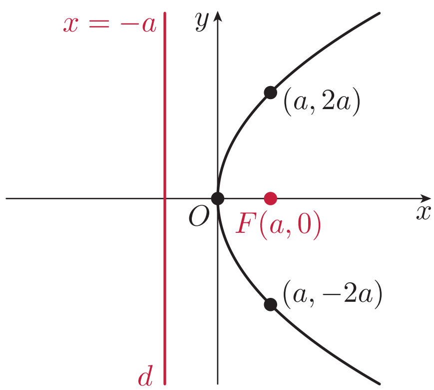


Figure 43 A parabola in standard position

As shown in Figure 43, the origin lies on a parabola in standard position, since it is equidistant from F and d; it is the **vertex** of the parabola. The x-axis is the **axis** of the parabola, since the parabola is symmetric with respect to this line.

The equation of a parabola in standard position with focus $(a, 0)$ can be expressed as

$$y^2 = 4ax.$$

Exercise A162

Sketch the parabola with equation $y^2 = 2x$.

Ellipse ($0 < e < 1$)

An ellipse with eccentricity e (where $0 < e < 1$) is the set of points P in the plane whose distances from a fixed point F are e times their distances from a fixed line d. An ellipse is in standard position if

- the focus F lies on the x-axis, with coordinates $(ae, 0)$, where $a > 0$
- the directrix d is the line with equation $x = a/e$.

An ellipse in standard position is symmetrical about the y-axis, so there is a second focus F_2 with coordinates $(-ae, 0)$, and a second directrix d_2 with equation $x = -a/e$. The features of an ellipse in standard position are shown in Figure 44.

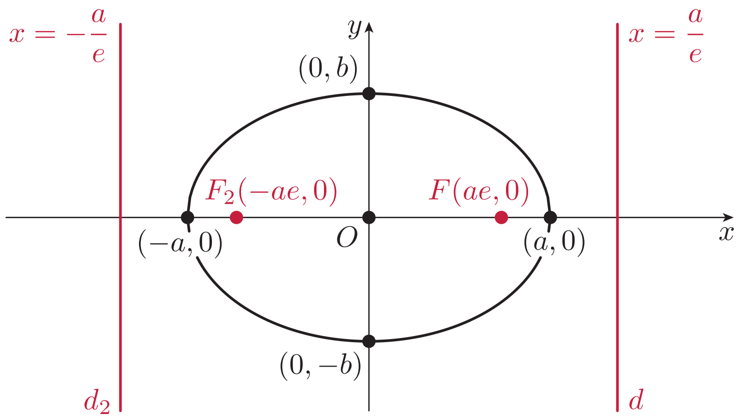


Figure 44 An ellipse in standard position

As shown in Figure 44, an ellipse in standard position intersects the x-axis at the points $(\pm a, 0)$, and intersects the y-axis at two points which we label $(0, \pm b)$. It can be shown that a and b are related to the eccentricity e of the ellipse by the equation

$$e = \sqrt{1 - \frac{b^2}{a^2}}.$$

The four points $(\pm a, 0)$ and $(0, \pm b)$ are the **vertices** of the ellipse. The origin is the **centre** of the ellipse. The largest width is along the x-axis, that is, $a > b > 0$. The line segment joining the points $(-a, 0)$ and $(a, 0)$ is the **major axis** of the ellipse, and the line segment joining the points $(0, -b)$ and $(0, b)$ is the **minor axis** of the ellipse.

The equation of an ellipse in standard position intersecting the x-axis at $(\pm a, 0)$ and the y-axis at $(0, \pm b)$, can be expressed as

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Exercise A163

Sketch the ellipse with equation $\dfrac{x^2}{3} + \dfrac{y^2}{2} = 1$, and find its eccentricity.

Hyperbola ($e > 1$)

A hyperbola is the set of points P in the plane whose distances from a fixed point F are e times their distances from a fixed line d, where $e > 1$. A hyperbola is in standard position if

- the focus F lies on the x-axis, with coordinates $(ae, 0)$, where $a > 0$
- the directrix d is the line with equation $x = a/e$.

A hyperbola in standard position is symmetrical about the y-axis, so there is a second focus F_2 with coordinates $(-ae, 0)$, and a second directrix d_2 with equation $x = -a/e$. The features of a hyperbola in standard position are shown in Figure 45.

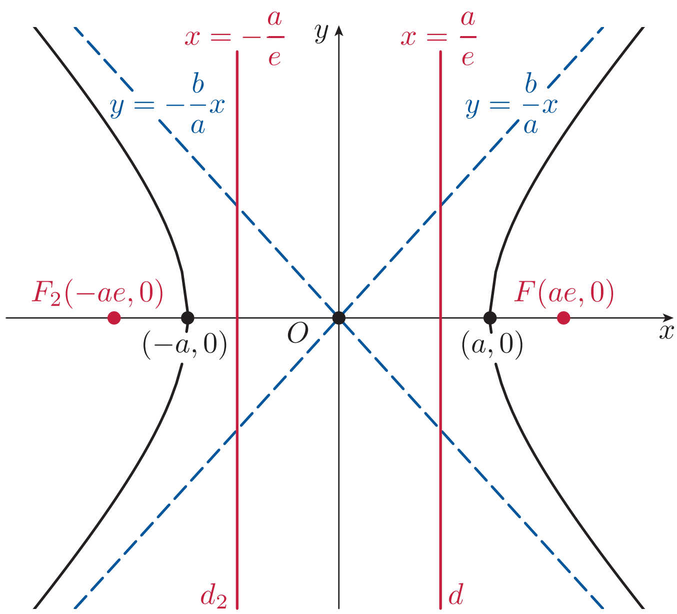


Figure 45 A hyperbola in standard position

As shown in Figure 45, a hyperbola in standard position intersects the x-axis at the points $(\pm a, 0)$, which are the **vertices** of the hyperbola. The origin is the **centre** of the hyperbola. The hyperbola has two asymptotes, which are lines passing through the origin. If we write the equations of these lines in the form

$$y = \pm\frac{b}{a}x,$$

then it can be shown that a and b are related to the eccentricity e of the hyperbola by the equation

$$e = \sqrt{1 + \frac{b^2}{a^2}}.$$

The equation of a hyperbola in standard position intersecting the x-axis at $(\pm a, 0)$ and with asymptotes $y = \pm(b/a)x$, can be expressed as

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

A hyperbola in standard position with $a = b$ has asymptotes $y = \pm x$, which are perpendicular lines. A hyperbola whose asymptotes are perpendicular is called a **rectangular hyperbola**. In Subsection 1.2 you saw that the graphs of linear rational functions are rectangular hyperbolas with asymptotes parallel to the x- and y-axes. An example of a rectangular hyperbola in standard position is shown in Figure 46.

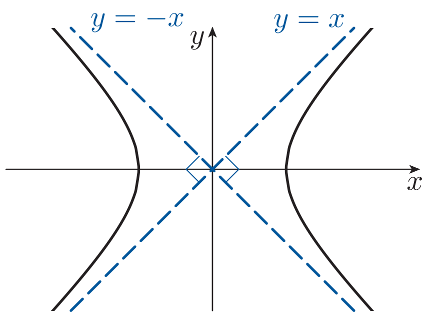


Figure 46 A rectangular hyperbola in standard position

Exercise A164

Sketch the hyperbola with equation $\dfrac{x^2}{3} - \dfrac{y^2}{2} = 1$ showing the asymptotes, and find its eccentricity.

5.3 General equation of a conic

The equation of a conic in standard position can always be expressed in the straightforward and easily recognisable forms given in the last subsection. However, not all conics are in standard position. In this subsection you will meet the general equation of a conic.

Let us begin by considering circles. In Unit A1 you saw that the equation of a circle with centre (a, b) and radius r is

$$(x-a)^2 + (y-b)^2 = r^2. \qquad (3)$$

For example, the equation

$$(x+1)^2 + (y-2)^2 = 3$$

represents a circle with centre $(-1, 2)$ and radius $\sqrt{3}$.

We can multiply out the brackets in this equation to get

$$x^2 + 2x + 1 + y^2 - 4y + 4 = 3,$$

that is,

$$x^2 + y^2 + 2x - 4y + 2 = 0.$$

In fact, if we have the equation of a circle in form (3), then we can always multiply out the brackets to write it in the alternative form

$$x^2 + y^2 + fx + gy + h = 0, \tag{4}$$

where f, g and h are real numbers. We may also choose to multiply through by a non-zero constant (for example, we might want to do this to avoid unpleasant fractions in the equation); this will give an equation of the form

$$ax^2 + ay^2 + fx + gy + h = 0, \tag{5}$$

where a is a non-zero constant and f, g and h are real numbers. Note that the coefficients of x^2 and y^2 are equal in this equation, and that the values of f, g and h will in general be different from those in equation (4).

Not every equation of this form represents a circle. For example, the equation $x^2 + y^2 + 1 = 0$ does not represent a circle since there are no points (x, y) satisfying it, and the equation $x^2 + y^2 = 0$ represents the single point $(0, 0)$. If we are given an equation of form (4) or (5), then we can determine whether it represents a circle, and, if so, find its centre and radius by using the method of completing the square, as demonstrated in the next worked exercise.

Worked Exercise A88

Show that the equation

$$x^2 + y^2 - 4x + 6y + 9 = 0$$

represents a circle, and find its centre and radius.

Solution

The equation can be rearranged as

$$x^2 - 4x + y^2 + 6y + 9 = 0.$$

Complete the square in the subexpression $x^2 - 4x$, then complete the square in the subexpression $y^2 + 6y$. Remember that to complete the square in the expression $x^2 + bx$, we write it as $(x + b/2)^2 - (b/2)^2$.

Completing the squares gives

$$((x - 2)^2 - 4) + ((y + 3)^2 - 9) + 9 = 0,$$

that is,

$$(x - 2)^2 + (y + 3)^2 = 4.$$

Therefore the equation represents the circle with centre $(2, -3)$ and radius $\sqrt{4} = 2$.

If you want to complete the square in an equation of form (5), where $a \neq 1$, then you can start by dividing through by a.

Exercise A165

For each of the following equations, determine whether it represents a circle, and, if it does, find the centre and radius of the circle.

(a) $x^2 + y^2 - 2x - 6y + 1 = 0$ (b) $x^2 + y^2 + x + y + 1 = 0$

(c) $x^2 + y^2 - 2x + 4y + 5 = 0$ (d) $2x^2 + 2y^2 + x - 3y - 5 = 0$

Now let us turn to conics in general. It can be shown that any conic, in any position in the plane, can be described by an equation of the form

$$Ax^2 + Bxy + Cy^2 + Fx + Gy + H = 0, \tag{6}$$

where A, B and C are not all zero.

Notice that when $A = C = 1$ and $B = 0$ equation (6) is the equation of a circle in form (4). Also, each of the (easily recognisable) equations of the non-degenerate conics in standard position can be rearranged to form (6):

$$y^2 = 4ax \quad \text{can be expressed as} \quad 4ax - y^2 = 0$$

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad \text{can be expressed as} \quad \frac{x^2}{a^2} + \frac{y^2}{b^2} - 1 = 0$$

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \quad \text{can be expressed as} \quad \frac{x^2}{a^2} - \frac{y^2}{b^2} - 1 = 0.$$

The equations of degenerate conics can also be expressed in form (6). For example:

- $x^2 + y^2 = 0$ represents the single point $(0, 0)$
- $x^2 - 2xy + y^2 = 0$ represents the single line $y = x$, since $x^2 - 2xy + y^2 = (x - y)^2$
- $x^2 - y^2 = 0$ represents the pair of lines $y = \pm x$ since $x^2 - y^2 = (x + y)(x - y)$.

Not every equation of form (6) represents a conic. For example, you have already seen that there are no points satisfying the equation $x^2 + y^2 + 1 = 0$, so in this case the equation describes the empty set. However, it turns out that every equation of form (6) represents *either* a conic *or* the empty set, so defining the empty set to be a degenerate conic yields the following theorem, which is stated without proof.

Theorem A18

Any conic has an equation of the form

$$Ax^2 + Bxy + Cy^2 + Fx + Gy + H = 0,$$

where A, B, C, F, G and H are real numbers, and A, B and C are not all zero. Conversely, the set of all points in $\mathbb{R}^2$ whose coordinates (x, y) satisfy an equation of this form is a conic.

Given the equation of a non-degenerate conic, such as

$$x^2 - 4xy - 2y^2 + 6x + 12y + 21 = 0,$$

we would like to be able to decide whether it represents an ellipse, a hyperbola or a parabola. (We know it is not a circle because of the non-zero term in xy.) A method of classifying non-degenerate conics from their equations will be established in Book C *Linear algebra*, where you will also meet the three-dimensional analogues of conics, which are known as *quadrics*.

5.4 Parametrising conics

Non-degenerate conics in standard position are not the graphs of functions, because for a *function*, each value of x in the domain must give rise to a *single* value of y in the codomain. For example, the unit circle is not the graph of a function, because if we take $x = 0$, for instance, then the equation $x^2 + y^2 = 1$ of the circle gives $y = 1$ and $y = -1$.

We can, however, describe a conic using a function f whose domain is an interval and whose codomain is $\mathbb{R}^2$. To do this, we define a function of the form

$$f : I \longrightarrow \mathbb{R}^2,$$

where I is an interval, such that the image set of f is the conic.

Such a function is called a *parametrisation* of the conic, and in this subsection you will see parametrisations for each different type of non-degenerate conic in standard position. First, however, we review the idea of parametrisation by applying it to lines in the plane.

Parametrising lines

In Subsection 2.5 of Unit A1 you saw that the following two sets are equal:

$$\{(x, y) \in \mathbb{R}^2 : 2x + y - 3 = 0\} \quad \text{and} \quad \{(t + 1, 1 - 2t) : t \in \mathbb{R}\}.$$

The equation $2x + y - 3 = 0$ can be rewritten as $y = 3 - 2x$, so the equality of the two sets above shows that, if

$$x = t + 1 \quad \text{and} \quad y = 1 - 2t, \tag{7}$$

then the point (x, y) traverses the whole line $y = 3 - 2x$ as t runs through all values in $\mathbb{R}$. Thus the function

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^2 \\ t &\longmapsto (t + 1, 1 - 2t) \end{aligned}$$

maps $\mathbb{R}$ to the line $y = 3 - 2x$. We say that t is a **parameter**, the equations (7) are **parametric equations** for the line, and the function f is a **parametrisation** of the line, which we can also write as

$$f(t) = (t + 1, 1 - 2t), \quad \text{for } t \in \mathbb{R}.$$

If we eliminate the parameter t by writing

$$t = x - 1,$$

we obtain

$$y = 1 - 2t = 1 - 2(x - 1) = 3 - 2x,$$

as expected.

Note that this parametrisation of the line $y = 3 - 2x$ is not unique. To see this, suppose we define another parametrisation g as follows:

$$g(t) = (2t, 3 - 4t), \quad \text{for } t \in \mathbb{R}.$$

This function corresponds to the parametric equations

$$x = 2t, \quad y = 3 - 4t.$$

Again, we can eliminate the parameter t by writing

$$t = x/2,$$

so

$$y = 3 - 4(x/2) = 3 - 2x,$$

as before. This shows that every point given by the parametrisation g is a point on the line $y = 3 - 2x$. On the other hand, if (a, b) is any point on the line $y = 3 - 2x$, then $b = 3 - 2a$, and for $t = a/2$ we have

$$g(t) = g(a/2) = (2(a/2), 3 - 4(a/2)) = (a, 3 - 2a) = (a, b),$$

so every point on the line $y = 3 - 2x$ corresponds to some value of t.

This shows that both parametrisations f and g give exactly the same line $y = 3 - 2x$. The difference between the two parametrisations is that the point (x, y) defined by the parametric equations traverses the line in different ways. Indeed, it is true in general that any line has many different parametrisations, where the line is traversed in different ways.

Exercise A166

(a) Sketch the line with the following parametrisation and find its equation in the form $y = mx + c$.

$$f(t) = (t + 1, t - 1) \quad \text{for } t \in \mathbb{R}.$$

(b) Show that

$$g(t) = (2t, 2t - 2) \quad \text{for } t \in \mathbb{R}$$

is another parametrisation of this line.

We now look at how to obtain a parametrisation of a (non-vertical) line given two points on it.

The line through any pair of points (p, q) and (r, s), where $r \neq p$, is given by

$$y - q = \frac{s - q}{r - p}(x - p). \tag{8}$$

To parametrise this line, we set

$t = (x - p)/(r - p)$. (You would not be expected to think of this!)

Rearranging gives $x = p + (r - p)t$.

Then substituting $t = (x - p)/(r - p)$ in equation (8) for the line gives

$$y - q = t(s - q) \quad \text{so} \quad y = q + (s - q)t.$$

These parametric equations

$$x = p + (r - p)t, \quad y = q + (s - q)t$$

correspond to the following parametrisation for this line

$$\alpha(t) = (p + (r - p)t, q + (s - q)t), \quad \text{for } t \text{ in } \mathbb{R},$$

as illustrated in Figure 47. Here the symbol α has been used for the parametrisation function; any symbol can be used.

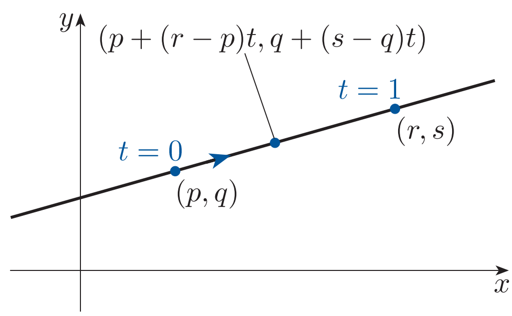


Figure 47 A parametrisation of the line though two points (p, q) and (r, s)

A parametrisation of a vertical line through the point $(p, 0)$ is

$$\alpha(t) = (p, t), \quad t \in \mathbb{R},$$

corresponding to the parametric equations

$$x = p, \quad y = t.$$

Exercise A167

Consider the line through the two points $(1, 2)$ and $(3, 6)$.

(a) Write down a parametrisation for this line.

(b) Which values of the parameter t correspond to the points $(2, 4)$, $(7, 14)$ and $(0, 0)$?

Circles

We now return to the question of how to parametrise conics, beginning with the unit circle.

By the definitions of the sine and cosine functions, if $P(x, y)$ is any point on the unit circle, and t is the angle in radians measured anticlockwise from the x-axis to the line OP, then

$$x = \cos t, \quad y = \sin t. \tag{9}$$

As the angle t increases from 0 to 2π, the point (x, y) travels once round the circle anticlockwise, starting and ending at the point $(1, 0)$, as shown in Figure 48. Note that even though $t = 0$ and $t = 2\pi$ give the same point, it is conventional to include both values in the range for this parametrisation. Thus the function

$$\begin{aligned} f : [0, 2\pi] &\longrightarrow \mathbb{R}^2 \\ t &\longmapsto (\cos t, \sin t) \end{aligned}$$

maps the interval $[0, 2\pi]$ to the unit circle, as shown in Figure 49.

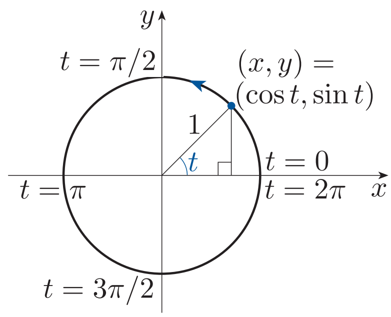


Figure 48 A point on the unit circle determined by the angle t

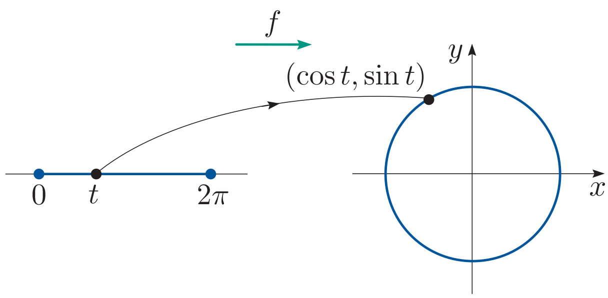


Figure 49 Mapping an interval to the unit circle

Equations (9) are parametric equations for the unit circle, and the function f is a parametrisation of the unit circle, which we can also write as

$$f(t) = (\cos t, \sin t), \quad t \in [0, 2\pi].$$

For this parametrisation, we can eliminate the parameter t by writing

$$x = \cos t \quad \text{and} \quad y = \sin t,$$

and using the trigonometric identity $\cos^2 t + \sin^2 t = 1$; this gives the equation $x^2 + y^2 = 1$, as expected.

Exercise A168

Mark on a sketch of the unit circle the coordinates of the points that correspond to the following values of the parameter t:

$$t = \pi/6, \quad t = \pi/2, \quad t = 3\pi/4, \quad t = \pi, \quad t = 3\pi/2, \quad t = 5\pi/3.$$

In general, the parametric equations for a curve have the form

$$x = f_1(t), \quad y = f_2(t),$$

where f_1 and f_2 are real functions of the parameter t. The functions f_1 and f_2 have the same domain, which is usually an interval.

For a single revolution of the circle, an appropriate interval is $[0, 2\pi]$, as we saw above. Another appropriate interval for the circle is $[-\pi, \pi]$, and a larger interval, such as $[0, 4\pi)$, will trace out the points of the circle more than once, in this case exactly twice each. Since a parametrisation is a function, every element in the domain must have a single image, but elements in the codomain may be the image of more than one element of the domain – the function need not be one-to-one. For example, in the case of the parametrisation of the unit circle using the interval $[0, 2\pi]$ given above, the values $t = 0$ and $t = 2\pi$ give the same point, $(1, 0)$.

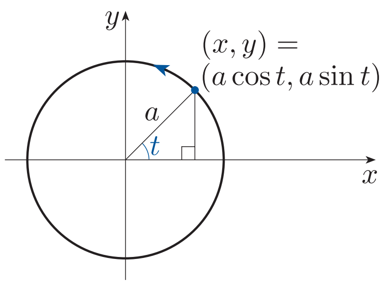


Figure 50 A parametrisation of a circle of radius a centred at the origin

So far you have seen a parametrisation of the unit circle; that is, the circle of radius 1 in standard position. For a circle of radius a in standard position, as shown in Figure 50, which has equation $x^2 + y^2 = a^2$, we can use the parametrisation

$$\alpha(t) = (a\cos t, a\sin t), \quad t \in [0, 2\pi];$$

this corresponds to the parametric equations

$$x = a\cos t, \quad y = a\sin t.$$

For the parametrisation above, we can eliminate the parameter t by writing

$$x/a = \cos t \quad \text{and} \quad y/a = \sin t,$$

and using the trigonometric identity $\cos^2 t + \sin^2 t = 1$; this gives the equation $x^2 + y^2 = a^2$, as expected.

To find a parametrisation of a circle of radius a centred at the point (p, q) we apply a (p, q)-translation to all the points on a circle of radius a centred at the origin. Thus a parametrisation of a circle of radius a centred at (p, q) is

$$x = p + a\cos t, \quad y = q + a\sin t, \quad t \in [0, 2\pi];$$

that is,

$$\alpha(t) = (p + a\cos t, q + a\sin t), \quad t \in [0, 2\pi].$$

Exercise A169

Write down a parametrisation for each of the following.

(a) The circle centred at the origin, with radius 3.

(b) The circle with centre $(2, 1)$ and radius 3.

Another parametrisation for the unit circle is

$$g(t) = (\cos 2\pi t, \sin 2\pi t), \quad t \in [0, 1]$$

which corresponds to the parametric equations

$$x = \cos 2\pi t, \quad y = \sin 2\pi t.$$

We have

$$x^2 + y^2 = \cos^2 2\pi t + \sin^2 2\pi t = 1,$$

so (x, y) is a point on the unit circle. As t increases from 0 to 1, $2\pi t$ increases from 0 to 2π, so the point (x, y) moves once round the circle.

You have now seen two different parametrisations for the unit circle traversed once anticlockwise – namely

$$f(t) = (\cos t, \sin t), \quad t \in [0, 2\pi],$$

and

$$g(t) = (\cos 2\pi t, \sin 2\pi t), \quad t \in [0, 1].$$

This illustrates the important fact that, just as you saw in the case of a line, a parametrisation of a given curve is not unique. Note that the point given by $g(t)$ moves round the unit circle 2π times more rapidly than the point given by $f(t)$. Different parametrisations of a curve may correspond to different modes of traversing the curve, and in general this may lead to a different starting point as well as a different pace or direction of travel.

In the remainder of this subsection we will briefly review the main features of the usual parametrisations for an ellipse, a parabola and a hyperbola in standard position.

Ellipse in standard position

For an ellipse in standard position, we use the parametrisation

$$\alpha(t) = (a \cos t, b \sin t), \quad t \in [0, 2\pi];$$

this gives the parametric equations

$$x = a \cos t, \quad y = b \sin t.$$

This parametrisation is illustrated in Figure 51.

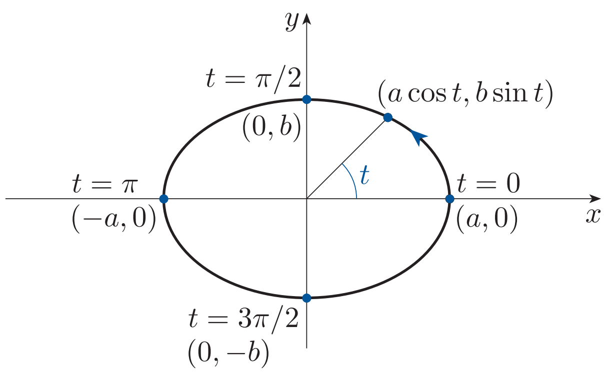


Figure 51 A parametrisation of an ellipse in standard position

For this parametrisation, we can eliminate the parameter t by writing

$$\frac{x}{a} = \cos t, \quad \frac{y}{b} = \sin t,$$

and using the trigonometric identity $\cos^2 t + \sin^2 t = 1$; this gives the equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

as expected.

When $b = a$, the equation reduces to that of the circle centred at the origin, with radius a; that is, $x^2 + y^2 = a^2$, as discussed above.

Parabola in standard position

For a parabola in standard position, we use the standard parametrisation

$$\alpha(t) = (at^2, 2at), \quad t \in \mathbb{R};$$

this gives the parametric equations

$$x = at^2, \quad y = 2at.$$

This parametrisation is illustrated in Figure 52.

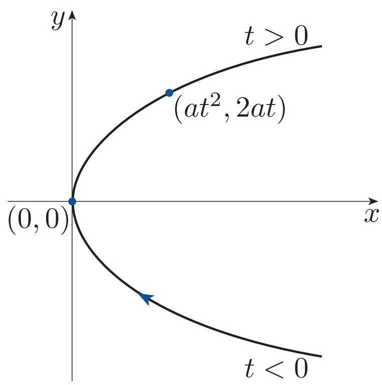


Figure 52 A parametrisation of a parabola in standard position

For this parametrisation, we can eliminate the parameter t by writing

$$y^2 = (2at)^2 = 4a^2t^2 = 4a \times at^2 = 4ax;$$

this gives $y^2 = 4ax$, as expected.

Hyperbola in standard position

For a hyperbola in standard position, we use the parametrisation

$$\alpha(t) = (a \sec t, b \tan t), \quad t \in [-\pi, \pi], \text{ excluding } -\pi/2 \text{ and } \pi/2;$$

this gives the parametric equations

$$x = a \sec t, \quad y = b \tan t.$$

The values $\pi/2$ and $-\pi/2$ are excluded since neither sec nor tan is defined at these angles.

This parametrisation is illustrated in Figure 53.

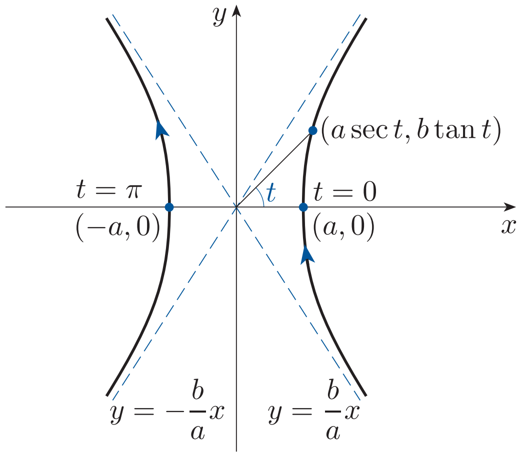


Figure 53 A parametrisation of a hyperbola in standard position

For this parametrisation, we can eliminate the parameter t by writing

$$\frac{x}{a} = \sec t, \quad \frac{y}{b} = \tan t,$$

and using the trigonometric identity $\sec^2 t - \tan^2 t = 1$; this gives the equation

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1,$$

as expected.

Exercise A170

Write down a parametrisation for each of the following conics.

(a) $y^2 = 2x$ (b) $\frac{x^2}{3} + \frac{y^2}{2} = 1$ (c) $\frac{x^2}{3} - \frac{y^2}{2} = 1$

(You sketched these conics in Exercises A162, A163 and A164, respectively.)

Exercise A171

Show that the points on the curve with parametrisation

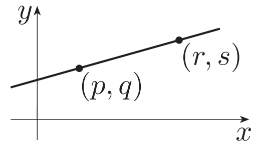
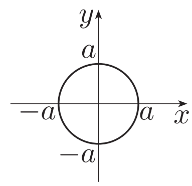
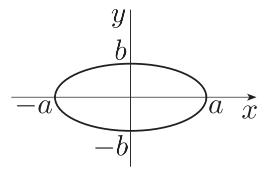
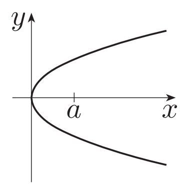
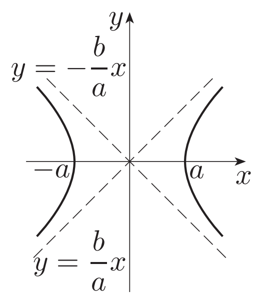
$$\alpha(t) = (a \cosh t, b \sinh t), \quad t \in \mathbb{R},$$

lie on the right-hand half of the hyperbola with equation $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$.

This hyperbolic parametrisation links the hyperbolic functions with the hyperbola from which their name arises.

5.5 Summary: some standard parametrisations

The following table gives a summary of the standard parametrisations for lines, circles and conics.

Line through (p, q) and (r, s) $y - q = \dfrac{s-q}{r-p}(x-p)$	$\alpha(t) = (p + (r-p)t, q + (s-q)t)$, for $t \in \mathbb{R}$	
Circle centre $(0, 0)$, radius a, $x^2 + y^2 = a^2$	$\alpha(t) = (a\cos t, a\sin t)$, for $t \in [0, 2\pi]$	
Ellipse in standard position $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$	$\alpha(t) = (a\cos t, b\sin t)$, for $t \in [0, 2\pi]$	
Parabola in standard position $y^2 = 4ax$	$\alpha(t) = (at^2, 2at)$, for $t \in \mathbb{R}$	
Hyperbola in standard position $\dfrac{x^2}{a^2} - \dfrac{y^2}{b^2} = 1$	$\alpha(t) = (a\sec t, b\tan t)$, for $t \in [-\pi, \pi]$, excluding $-\pi/2$ and $\pi/2$ or $\alpha(t) = (a\cosh t, b\sinh t)$, for $t \in \mathbb{R}$ (right-hand half only)	

Summary

In this unit, you have seen how the properties of a real function can be analysed and represented using its graph. You have learned to recognise and sketch the graphs of basic real functions, including some whose graphs are smooth curves everywhere in their domains and others whose graphs have 'corners' or 'jumps' (for example, the modulus function). You have then seen how the graphs of basic functions are modified under translations or scalings, and met a strategy for sketching the graphs of more complicated real functions by looking at how various properties of functions affect their graphs.

You have met the hyperbolic functions and seen that these functions are related to the exponential function, but have many properties analogous to the trigonometric functions, though they are not periodic. Finally, you have studied conic sections and seen how they can be expressed in the form of a function $f : \mathbb{R} \longrightarrow \mathbb{R}^2$, known as a parametrisation of the conic.

You will continue your study of real functions in the analysis units of this module.

Learning outcomes

After working through this unit, you should be able to:

- recognise and use the graphs of the basic real functions
- understand the effect on a graph of *translations* and *scalings*
- understand how the shape of a graph of a function indicates properties of the function, such as its being *increasing*, *decreasing*, *even* or *odd*
- use the rule of a function to determine the main features of its graph as listed in the graph-sketching strategies
- sketch the graphs of a variety of real functions
- sketch the graph of a *hybrid function*, whose rule is defined by different formulas on different parts of its domain
- define the *hyperbolic functions* $\cosh x$, $\sinh x$ and $\tanh x$, and be familiar with their properties
- sketch the graphs of $\cosh x$, $\sinh x$ and $\tanh x$, and their reciprocals
- explain the term *conic section*, and the *focus–directrix definitions* of the non-degenerate conics
- sketch a conic in standard position from its equation
- obtain the equations of lines and conics in standard position from their parametric representations.

Solutions to exercises

Solution to Exercise A138

(a) The denominator of $f(x)$ is $1 - x^2$, which is zero when $x = 1$ or -1, so the domain is the set $\mathbb{R} - \{-1, 1\}$ (that is, the set of all real numbers, excluding -1 and 1).

(b) This function is defined for all real numbers, so the domain is $\mathbb{R}$.

(c) The denominator of $f(x)$ is $x^2 + 5x + 4 = (x+1)(x+4)$, which is zero when $x = -1$ or -4, so the domain is the set $\mathbb{R} - \{-1, -4\}$.

(d) The denominator of $f(x)$ is $\sqrt{1 - x^2}$, which is zero when $x = 1$ or -1, and is not defined when $x^2 > 1$, that is, when $x > 1$ or $x < -1$, so the domain is the interval $(-1, 1)$.

Solution to Exercise A139

(a) $(-\infty, -1) \cup (-1, 1) \cup (1, \infty)$

(b) $\mathbb{R} = (-\infty, \infty)$

(c) $(-\infty, -4) \cup (-4, -1) \cup (-1, \infty)$

(d) $(-1, 1)$

Solution to Exercise A140

(a) We have
$$\begin{aligned} f(x) &= 2x^2 - 8x + 11 \\ &= 2(x^2 - 4x) + 11 \\ &= 2((x-2)^2 - 4) + 11 \\ &= 2(x-2)^2 + 3. \end{aligned}$$

Hence the parabola has vertex $(2, 3)$. So it is graph B. (Since the coefficient of x^2 is positive, the parabola is the same way up as the graph of $y = x^2$.)

(b) We have
$$\begin{aligned} f(x) &= -2x^2 - 8x - 5 \\ &= -2(x^2 + 4x) - 5 \\ &= -2((x+2)^2 - 4) - 5 \\ &= -2(x+2)^2 + 3. \end{aligned}$$

Hence the parabola has vertex $(-2, 3)$. Since the coefficient of x^2 is negative, the parabola is the opposite way up to the graph of $y = x^2$. So it is graph D.

(c) We have
$$\begin{aligned} f(x) &= -2x^2 - 8x - 11 \\ &= -2(x^2 + 4x) - 11 \\ &= -2((x+2)^2 - 4) - 11 \\ &= -2(x+2)^2 - 3. \end{aligned}$$

Hence the parabola has vertex $(-2, -3)$. So it is graph C. (Since the coefficient of x^2 is negative, the parabola is the opposite way up to the graph of $y = x^2$.)

(d) We have
$$\begin{aligned} f(x) &= 2x^2 + 8x + 11 \\ &= 2(x^2 + 4x) + 11 \\ &= 2((x+2)^2 - 4) + 11 \\ &= 2(x+2)^2 + 3. \end{aligned}$$

Hence the parabola has vertex $(-2, 3)$. Since the coefficient of x^2 is positive, the parabola is the same way up as the graph of $y = x^2$. So it is graph A.

Solution to Exercise A141

(a) Linear: 1, 22.

(b) Quadratic: 2, 11, 21.

(c) Cubic: 8, 15.

(d) Trigonometric: 5, 6, 16, 19.

(e) Linear rational: 7, 13.

(f) Modulus (or related): 4, 10, 18.

(g) Integer part (or related): 9, 23.

(h) Exponential (or related): 12, 20.

(i) Not the graph of y as some function of x: 3, 14, 17, 24.

Solution to Exercise A142

(a) The graph of $y = \cos(x/2)$ is obtained from the graph of $y = \cos x$ by a $(2, 1)$-scaling. This is graph D.

(b) The graph of $y = 2\cos x$ is obtained from the graph of $y = \cos x$ by a $(1, 2)$-scaling. This is graph C.

(c) The graph of $y = 2\cos 2x$ is obtained from the graph of $y = \cos x$ by a $\left(\frac{1}{2}, 2\right)$-scaling. This is graph A.

(d) The graph of $y = \frac{1}{2}\cos x$ is obtained from the graph of $y = \cos x$ by a $\left(1, \frac{1}{2}\right)$-scaling. This is graph B.

Solution to Exercise A143

(a) The graph of $y = (x-2)^2 + 1$ is obtained from the graph of $y = x^2$ by a $(2, 1)$-translation. This is graph C.

(b) The graph of $y = (x+2)^2 + 1$ is obtained from the graph of $y = x^2$ by a $(-2, 1)$-translation. This is graph D.

(c) The graph of $y = -(x-2)^2 + 1$ is obtained from the graph of $y = x^2$ by applying both a scaling and a translation.

Consider $y = x^2$ and multiply the right-hand side by -1 to obtain the equation $y = -x^2$. Then replace x by $x - 2$ to obtain the equation $y = -(x-2)^2$ and finally add 1 to the right-hand side of this equation to obtain $y = -(x-2)^2 + 1$.

So the graph of $-(x-2)^2 + 1$ is obtained from the graph of $y = x^2$ by a $(1, -1)$-scaling followed by a $(2, 1)$-translation. This is graph B.

(d) The graph of $y = (x-2)^2 - 1$ is obtained from the graph of $y = x^2$ by a $(2, -1)$-translation. This is graph A.

Solution to Exercise A144

(a) B and E are graphs of odd functions.

(b) A and F are graphs of even functions.

(c) C and D are graphs of functions that are neither odd nor even.

Solution to Exercise A145

(a)
$$\begin{aligned} x^2 - 6x + 11 &= (x-3)^2 - 9 + 11 \\ &= (x-3)^2 + 2 \end{aligned}$$

which is always positive.

(b)
$$\begin{aligned} 3x^2 + 12x - 1 &= 3(x^2 + 4x) - 1 \\ &= 3\left((x+2)^2 - 4\right) - 1 \\ &= 3(x+2)^2 - 12 - 1 \\ &= 3(x+2)^2 - 13 \end{aligned}$$

which is sometimes positive and sometimes negative (for example, positive when $x = 1$ and negative when $x = 0$).

Solution to Exercise A146

(a) A is the graph of a function that is increasing but not strictly increasing.

(b) E is the graph of a function that is strictly increasing.

(c) F is the graph of a function that is decreasing but not strictly decreasing.

(d) C is the graph of a function that is strictly decreasing.

(e) B and D are graphs of functions that are increasing on part of the domain and decreasing on another part of the domain.

Solution to Exercise A147

$$\begin{aligned} f'(x) &= 4x^3 - 4x \\ &= 4x(x^2 - 1) \\ &= 4x(x-1)(x+1). \end{aligned}$$

We construct a table of signs for f'. To save space, we omit the first and last interval headings.

x		-1	$(-1, 0)$	0	$(0, 1)$	1	
$4x$	$-$	$-$	$-$	0	$+$	$+$	$+$
$x-1$	$-$	$-$	$-$	$-$	$-$	0	$+$
$x+1$	$-$	0	$+$	$+$	$+$	$+$	$+$
$f'(x)$	$-$	0	$+$	0	$-$	0	$+$

Thus

- f is increasing on the intervals $(-1, 0)$ and $(1, \infty)$
- f is decreasing on the intervals $(-\infty, -1)$ and $(0, 1)$
- f has stationary points at $x = -1,\ 0$ and 1.

By the First Derivative Test, we deduce that

- there is a local minimum at $x = -1$ with $f(-1) = 2$
- there is a local maximum at $x = 0$ with $f(0) = 3$
- there is a local minimum at $x = 1$ with $f(1) = 2$.

Solution to Exercise A148

$f(x) \to \infty$ as $x \to 1^-$
$f(x) \to -\infty$ as $x \to 1^+$
$f(x) \to 0$ as $x \to \infty$
$f(x) \to 0$ as $x \to -\infty$.

Solution to Exercise A149

(a) $f(x) \to \infty$ as $x \to \pm\infty$.

(b) $f(x) \to \infty$ as $x \to \infty$
$f(x) \to -\infty$ as $x \to -\infty$.

(c) $f(x) \to -\infty$ as $x \to \pm\infty$.

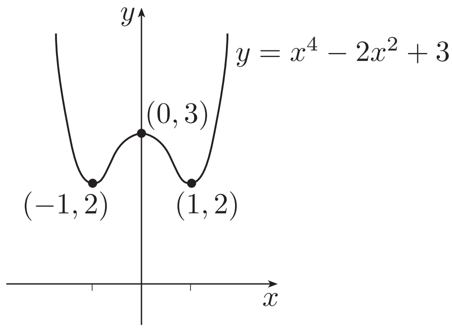
(d) $f(x) \to -\infty$ as $x \to \infty$
$f(x) \to \infty$ as $x \to -\infty$.

Solution to Exercise A150

$f(x) = x^4 - 2x^2 + 3$.

1. The domain of f is $\mathbb{R}$.
2. f is even, since, for all x in $\mathbb{R}$,
$$f(-x) = (-x)^4 - 2(-x)^2 + 3$$
$$= x^4 - 2x^2 + 3 = f(x).$$
3. Using the hint and completing the square we get $t^2 - 2t + 3 = (t-1)^2 - 1 + 3$, so
$$f(x) = (x^2 - 1)^2 + 2 \geq 2$$
for all x in $\mathbb{R}$, so f is positive on $\mathbb{R}$. This means that f has no x-intercepts, as $f(x)$ is never zero. The y-intercept is $f(0) = 3$.
4. By step 3, f is positive on $\mathbb{R}$.
5. In Exercise A147 you found that
   - f is increasing on the intervals $(-1, 0)$ and $(1, \infty)$
   - f is decreasing on the intervals $(-\infty, -1)$ and $(0, 1)$
   - f has stationary points at $x = -1$, 0 and 1
   - there is a local minimum at $x = -1$ with $f(-1) = 2$
   - there is a local maximum at $x = 0$ with $f(0) = 3$
   - there is a local minimum at $x = 1$ with $f(1) = 2$.
6. The power of x in the dominant term is even and its coefficient is positive, so
$$f(x) \to \infty, \quad \text{as } x \to \pm\infty.$$

This information enables us to sketch the graph.



Solution to Exercise A151

$$f(x) = \frac{x-3}{2-x}.$$

1. The domain of f is $\mathbb{R} - \{2\}$.
2. f is neither even nor odd, since its domain is not symmetric about the origin.
3. We have $f(x) = 0$ only when $x = 3$, so the only x-intercept is 3.

   The y-intercept is $f(0) = -\frac{3}{2}$.
4. We construct a table of signs for f.

x	$(-\infty, 2)$	2	$(2, 3)$	3	$(3, \infty)$
$x - 3$	$-$	$-$	$-$	0	$+$
$2 - x$	$+$	0	$-$	$-$	$-$
$f(x)$	$-$	$*$	$+$	0	$-$

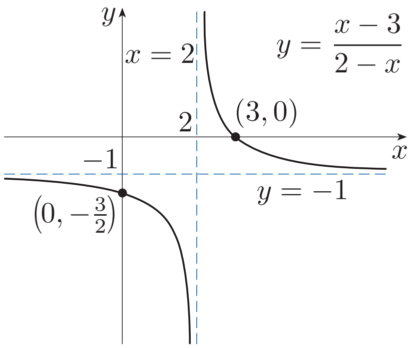
   Thus
   - f is positive on the interval $(2, 3)$
   - f is negative on the intervals $(-\infty, 2)$ and $(3, \infty)$.
5. Using the quotient rule,
$$f'(x) = \frac{(2-x) + (x-3)}{(2-x)^2} = \frac{-1}{(2-x)^2},$$
so $f'(x) < 0$ for all x in the domain; that is, f is decreasing on each interval of its domain.
6. The denominator is 0 when $x = 2$, so the line $x = 2$ is a vertical asymptote.

Also, by step 4,

$$f(x) \to -\infty, \quad \text{as } x \to 2^-,$$
$$f(x) \to \infty, \quad \text{as } x \to 2^+.$$

The dominant term of the numerator is x and the dominant term of the denominator is $-x$. Thus the power of x is the same in each dominant term. The ratio of the coefficients of the dominant terms is -1. Therefore the line $y=-1$ is a horizontal asymptote.

This information enables us to sketch the graph.



Solution to Exercise A152

$$f(x) = \frac{1}{x(x+1)^2}.$$

1. The domain of f is $\mathbb{R} - \{0, -1\}$.
2. f is neither even nor odd, since the domain is not symmetric about 0.
3. The equation $f(x) = 0$ has no solution, so there are no x-intercepts.

   $f(0)$ is not defined, so there is no y-intercept.
4. We construct a table of signs for f.

x	$(-\infty,-1)$	-1	$(-1,0)$	0	$(0,\infty)$
x	$-$	$-$	$-$	0	$+$
$(x+1)^2$	$+$	0	$+$	$+$	$+$
$f(x)$	$-$	$*$	$-$	$*$	$+$

   Thus

   - f is positive on the interval $(0,\infty)$
   - f is negative on the intervals $(-\infty,-1)$ and $(-1,0)$.

5. Using the quotient and product rules,

$$f'(x) = -\frac{(x+1)^2 + 2x(x+1)}{x^2(x+1)^4}$$
$$= -\frac{(x+1)(x+1+2x)}{x^2(x+1)^4}$$
$$= -\frac{3x+1}{x^2(x+1)^3},$$

   so

$$f'(x) = 0 \text{ when } x = -\tfrac{1}{3}.$$

   We construct a table of signs for f'.

x		-1	$(-1,-\frac{1}{3})$	$-\frac{1}{3}$	$(-\frac{1}{3},0)$	0	
$-(3x+1)$	$+$	$+$	$+$	0	$-$	$-$	$-$
x^2	$+$	$+$	$+$	$+$	$+$	0	$+$
$(x+1)^3$	$-$	0	$+$	$+$	$+$	$+$	$+$
$f'(x)$	$-$	$*$	$+$	0	$-$	$*$	$-$

   We deduce that

   - f is increasing on the interval $\left(-1,-\frac{1}{3}\right)$
   - f is decreasing on the intervals $(-\infty,-1)$, $\left(-\frac{1}{3},0\right)$ and $(0,\infty)$
   - f has a stationary point at $x=-\frac{1}{3}$.

   By the First Derivative Test, we deduce that there is a local maximum at $x=-\frac{1}{3}$. We have $f\left(-\frac{1}{3}\right) = -\frac{27}{4}$.

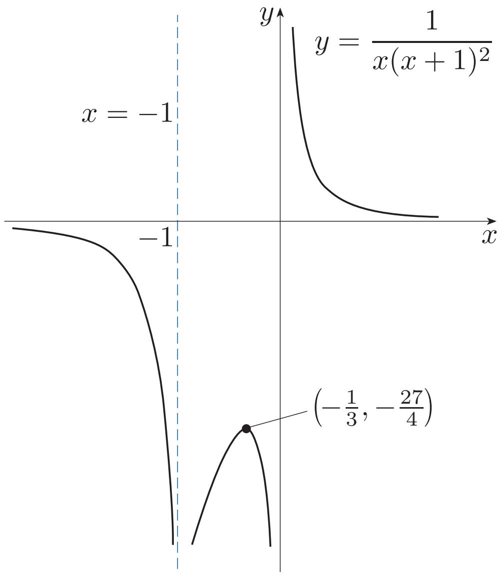
6. The denominator is 0 when $x=0$ or $x=-1$, so the lines $x=0$ and $x=-1$ are vertical asymptotes.

   Also, by step 4,

$$f(x) \to -\infty \quad \text{as } x \to -1^-$$
$$f(x) \to -\infty \quad \text{as } x \to -1^+$$
$$f(x) \to -\infty \quad \text{as } x \to 0^-$$
$$f(x) \to \infty \quad \text{as } x \to 0^+.$$

   The power of x in the dominant term in the numerator (0, since $1 = x^0$) is less than the power of x in the dominant term of the denominator (3), so the line $y=0$ is a horizontal asymptote. (Alternatively, by steps 4 and 5, $f(x) \to 0$ as $x \to \pm\infty$.)

This information enables us to sketch the graph.

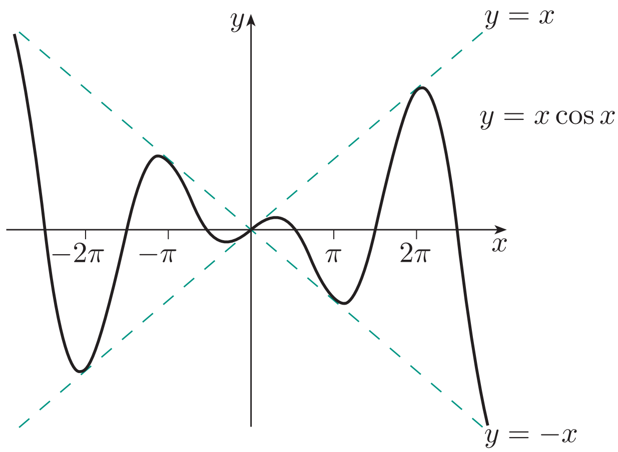


Solution to Exercise A153

$f(x) = x\cos x$.

1. The function f has domain $\mathbb{R}$, since both x and $\cos x$ have domain $\mathbb{R}$.
2. The function f is odd, since for all x in $\mathbb{R}$,
$$\begin{aligned} f(-x) &= -x\cos(-x) \\ &= -x\cos x = -f(x). \end{aligned}$$
We consider the features of the graph of f for $x \geq 0$, and then rotate the graph we obtain through π about the origin.
Although f involves a trigonometric function, it is not periodic because of the factor of x.
3. We have $f(x) = 0$ when $x = 0$ or when $\cos x = 0$.
So the x-intercepts are $0, \pi/2, 3\pi/2, \ldots$.
The y-intercept is 0 since $f(0) = 0$.
4. The intervals on which f is positive or negative (for $x > 0$) alternate between the x-intercepts in the same way as for the cosine function.
For $x > 0$,
   - f is positive on $(0, \pi/2), (3\pi/2, 5\pi/2), (7\pi/2, 9\pi/2), \ldots$,
   - f is negative on $(\pi/2, 3\pi/2), (5\pi/2, 7\pi/2), \ldots$.
5. $f'(x) = \cos x - x\sin x$, so we omit solving $f'(x) = 0$, as it is not easy.
6. The function f has no asymptotes.
7. Since $-1 \leq \cos x \leq 1$ for all real numbers x, we have
$$-x \leq x\cos x \leq x, \quad \text{for } x > 0.$$
That is,
$$-x \leq f(x) \leq x, \quad \text{for } x > 0,$$
so, for $x > 0$, the graph of f lies between the lines $y = x$ and $y = -x$. These are the construction lines for this function.
The function f, for $x > 0$, has the following features:
$$f(x) = x \text{ when } \cos x = 1$$
$$f(x) = -x \text{ when } \cos x = -1.$$
For $x > 0$, the graph of f
   - meets the construction line $y = x$ when $x = 2\pi, 4\pi, 6\pi \ldots$
   - meets the construction line $y = -x$ when $x = \pi, 3\pi, 5\pi \ldots$.

This information enables us to sketch the graph.



Solution to Exercise A154

$f(x) = x + \sin x$.

1. The function f has domain $\mathbb{R}$, since both x and $\sin x$ have domain $\mathbb{R}$.
2. $x + \sin x$ is odd, since for all x in $\mathbb{R}$,
$$\begin{aligned} f(-x) &= -x + \sin(-x) \\ &= -(x + \sin x) = -f(x). \end{aligned}$$
We consider the features of the graph of f for $x \geq 0$, and then rotate the graph we obtain through π about the origin.

Although f involves a trigonometric function, it is not periodic because of the addition of x.

3. We have $f(0) = 0$, so 0 is both the x-intercept and the y-intercept. There are no other values of x for which $f(x) = 0$.
4. f is positive on $(0, \infty)$.
5. $f'(x) = 1 + \cos x$, so $f'(x) = 0$ when $\cos x = -1$, that is, when $x = (2k+1)\pi$, for any integer k.

   At all other points in $(0, \infty)$, $f'(x) > 0$, so

   - f is increasing on $(0, \infty)$
   - f has stationary points when $x = \pi, 3\pi, 5\pi, \ldots$.

   By the First Derivative Test, we deduce that there is a horizontal point of inflection when $x = \pi, 3\pi, 5\pi, \ldots$.

   We have $f(\pi) = \pi$, $f(3\pi) = 3\pi$, $\ldots$.
6. The function has no asymptotes.
7. Since $-1 \leq \sin x \leq 1$ for all real numbers x, we have

   $$x - 1 \leq x + \sin x \leq x + 1, \quad \text{for } x > 0.$$

   That is,

   $$x - 1 \leq f(x) \leq x + 1, \quad \text{for } x > 0,$$

   so, for $x > 0$, the graph of f lies between the graphs of the functions $y = x - 1$ and $y = x + 1$.

   The function f, for $x > 0$, has the following features:

   $$f(x) = x \text{ when } \sin x = 0$$

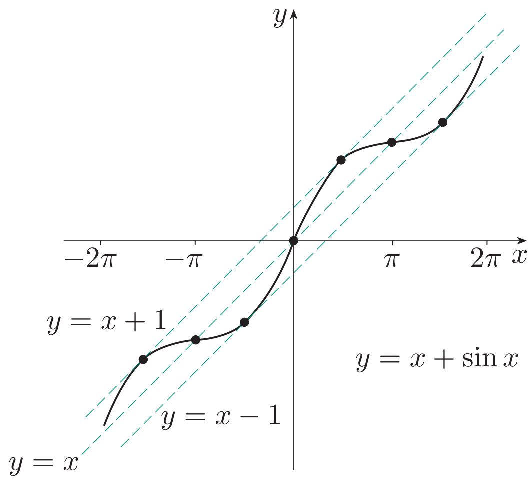
   $$f(x) = x + 1 \text{ when } \sin x = 1$$

   $$f(x) = x - 1 \text{ when } \sin x = -1.$$

   So $y = x$, $y = x + 1$ and $y = x - 1$ can be used as construction lines, and for $x > 0$, the graph of f

   - meets the construction line $y = x$ when $x = 0, \pi, 2\pi, \ldots$
   - meets the construction line $y = x + 1$ when $x = \pi/2, 5\pi/2, 9\pi/2, \ldots$
   - meets the construction line $y = x - 1$ when $x = 3\pi/2, 7\pi/2, 11\pi/2, \ldots$.

This information enables us to sketch the graph.



Solution to Exercise A155

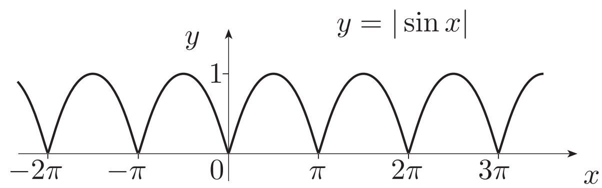
The modulus function maps any negative number to its corresponding positive value, so the zeros of f are exactly those of $\sin x$, and for each interval on which

- $\sin x$ is positive, we have $f(x) = \sin x$
- $\sin x$ is negative, we reflect in the x-axis to get $f(x) = |\sin x|$.

And for any integer k, there are

- local maxima with value 1 at $x = \frac{1}{2}(2k+1)\pi$
- local minima with value 0 at $x = k\pi$.

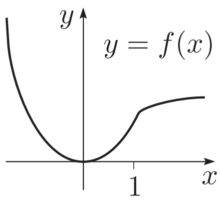
We therefore obtain the following graph.



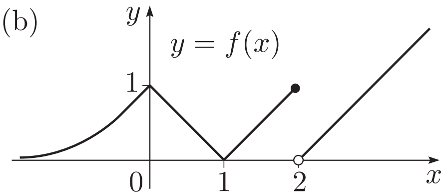
Solution to Exercise A156

Each of these functions has domain $\mathbb{R}$.

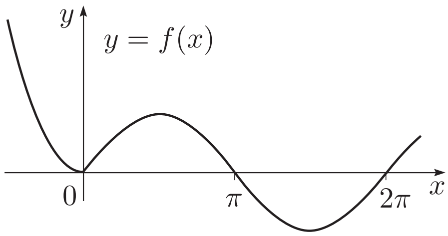
(a)



(b)



(c)



Solution to Exercise A157

(a) $e^x(e^x + e^{-x}) = e^{2x} + e^0$
$= e^{2x} + 1$

(b) $(e^{2x} - e^{-2x})/e^x = e^x - e^{-3x}$

(c) $(e^{5x} + e^{-5x})(e^{5x} - e^{-5x})$
$= e^{10x} - e^0 + e^0 - e^{-10x}$
$= e^{10x} - e^{-10x}$

Solution to Exercise A158

(a) $\cosh^2 x - \sinh^2 x$

$$\begin{aligned}
&= \tfrac{1}{4}(e^x + e^{-x})^2 - \tfrac{1}{4}(e^x - e^{-x})^2 \\
&= \tfrac{1}{4}(e^{2x} + 2e^x e^{-x} + e^{-2x}) \\
&\quad - \tfrac{1}{4}(e^{2x} - 2e^x e^{-x} + e^{-2x}) \\
&= \tfrac{1}{4}(e^{2x} + 2 + e^{-2x} - e^{2x} + 2 - e^{-2x}) \\
&= \tfrac{1}{4} \times 4 = 1
\end{aligned}$$

(b) $\cosh x \cosh y + \sinh x \sinh y$

$$\begin{aligned}
&= \tfrac{1}{2}(e^x + e^{-x})\tfrac{1}{2}(e^y + e^{-y}) \\
&\quad + \tfrac{1}{2}(e^x - e^{-x})\tfrac{1}{2}(e^y - e^{-y}) \\
&= \tfrac{1}{4}(e^x e^y + e^x e^{-y} + e^{-x} e^y + e^{-x} e^{-y}) \\
&\quad + \tfrac{1}{4}(e^x e^y - e^x e^{-y} - e^{-x} e^y + e^{-x} e^{-y}) \\
&= \tfrac{1}{4}(e^{x+y} + e^{x-y} + e^{-x+y} + e^{-(x+y)}) \\
&\quad + \tfrac{1}{4}(e^{x+y} - e^{x-y} - e^{-x+y} + e^{-(x+y)}) \\
&= \tfrac{1}{2}(e^{x+y} + e^{-(x+y)}) \\
&= \cosh(x + y)
\end{aligned}$$

(c) $\sinh x \cosh y + \cosh x \sinh y$

$$\begin{aligned}
&= \tfrac{1}{2}(e^x - e^{-x})\tfrac{1}{2}(e^y + e^{-y}) \\
&\quad + \tfrac{1}{2}(e^x + e^{-x})\tfrac{1}{2}(e^y - e^{-y}) \\
&= \tfrac{1}{4}(e^x e^y + e^x e^{-y} - e^{-x} e^y - e^{-x} e^{-y}) \\
&\quad + \tfrac{1}{4}(e^x e^y - e^x e^{-y} + e^{-x} e^y - e^{-x} e^{-y}) \\
&= \tfrac{1}{4}(e^{x+y} + e^{x-y} - e^{-x+y} - e^{-(x+y)}) \\
&\quad + \tfrac{1}{4}(e^{x+y} - e^{x-y} + e^{-x+y} - e^{-(x+y)}) \\
&= \tfrac{1}{2}(e^{x+y} - e^{-(x+y)}) \\
&= \sinh(x + y)
\end{aligned}$$

Solution to Exercise A159

Let $f(x) = \cosh x = \frac{1}{2}(e^x + e^{-x})$; then

$$f'(x) = \tfrac{1}{2}(e^x - e^{-x}) = \sinh x.$$

Let $g(x) = \sinh x = \frac{1}{2}(e^x - e^{-x})$; then

$$g'(x) = \tfrac{1}{2}(e^x + e^{-x}) = \cosh x.$$

Thus

$$\cosh' = \sinh \quad \text{and} \quad \sinh' = \cosh\,.$$

These are similar to the trigonometric derivatives

$$\cos' = -\sin \quad \text{and} \quad \sin' = \cos,$$

but differ by a minus sign in the first one.

Solution to Exercise A160

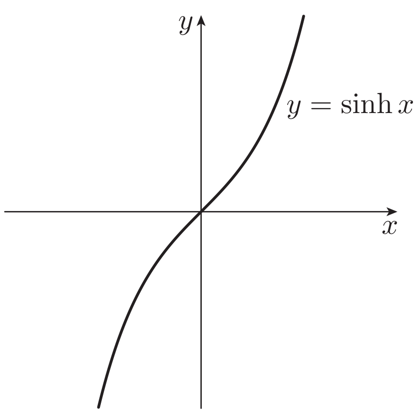
$f(x) = \sinh x$.

1. $\sinh x$ has domain $\mathbb{R}$.
2. $\sinh x$ is odd, since
$$\begin{aligned} f(-x) &= \sinh(-x) \\ &= \tfrac{1}{2}(e^{-x} - e^{-(-x)}) \\ &= \tfrac{1}{2}(e^{-x} - e^{x}) \\ &= -\tfrac{1}{2}(e^{x} - e^{-x}) \\ &= -\sinh x = -f(x). \end{aligned}$$
It is therefore sufficient to consider the features of the graph of f for $x \geq 0$, and then to rotate the graph we obtain through π about the origin.
3. $\sinh x = \frac{1}{2}(e^x - e^{-x}) = 0$ when $e^x = e^{-x}$; so the only zero of $\sinh x$ is 0.

   So 0 is both the x-intercept and the y-intercept.
4. From the graphs of $y = e^x$ and $y = e^{-x}$, we observe that $\sinh x$ is positive for $x > 0$.
5. We know that $\sinh' x = \cosh x$, and also, for all x in $\mathbb{R}$, that $\cosh x \geq 1$, so $\sinh x$ is strictly increasing on $\mathbb{R}$, and so has no stationary points.

   (Since $\sinh' x = \cosh x$ and $\cosh 0 = 1$, the graph of $\sinh x$ has gradient 1 at the origin.)
6. Since $e^x \to \infty$ as $x \to \infty$ and $e^{-x} \to 0$ as $x \to \infty$,
$$\sinh x \to \infty \quad \text{as } x \to \infty.$$

This information enables us to sketch the graph.



Solution to Exercise A161

$$\operatorname{cosech} x = \frac{1}{\sinh x}.$$

1. $\sinh x = 0$ when $x = 0$, so $\operatorname{cosech} x$ is not defined at 0. Thus $\operatorname{cosech} x$ has domain $\mathbb{R}$, excluding 0.
2. $\operatorname{cosech} x$ is odd, since $\sinh x$ is odd. It is therefore sufficient to consider the features of the graph of f for $x > 0$, and then to rotate the graph we obtain through π about the origin.

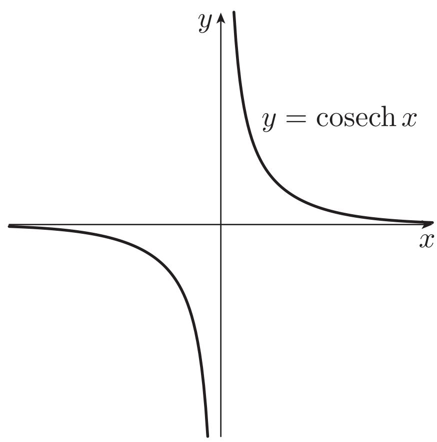
3 and 4. We know that $\sinh x > 0$ for $x > 0$, so $\operatorname{cosech} x > 0$ for $x > 0$, thus $\operatorname{cosech} x$ has no zeros since $\operatorname{cosech} x$ is not defined at $x = 0$, it has neither x-intercepts nor y-intercepts.

5. We know $\sinh x$ is increasing on $\mathbb{R}$, so
   - $\operatorname{cosech} x$ is decreasing on $(0, \infty)$
   - $\operatorname{cosech} x$ has no local maxima or local minima.
6. We know that when $x = 0$, $\sinh x = 0$ and that $\sinh x \to \infty$ as $x \to \infty$.

   Since $\operatorname{cosech} x = 1/\sinh x$, and $\sinh x$ is small when x is close to 0, the line $x = 0$ is a vertical asymptote.

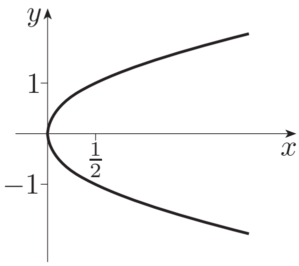
   From steps 3 and 4, we know that
$$\operatorname{cosech} x \to \infty \quad \text{as } x \to 0^+.$$
   Also,
$$\operatorname{cosech} x \to 0 \quad \text{as } x \to \infty.$$

This information enables us to sketch the graph.



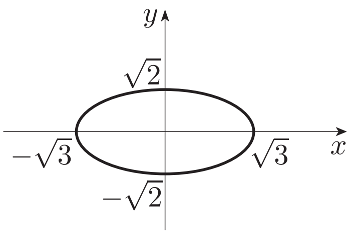
Solution to Exercise A162

The parabola $y^2 = 4ax$ has focus $(a, 0)$, so the parabola $y^2 = 2x$ has focus $(1/2, 0)$.



Solution to Exercise A163

We have $a^2 = 3$ and $b^2 = 2$, so $a = \sqrt{3}$ and $b = \sqrt{2}$. The ellipse with equation $\dfrac{x^2}{3} + \dfrac{y^2}{2} = 1$.



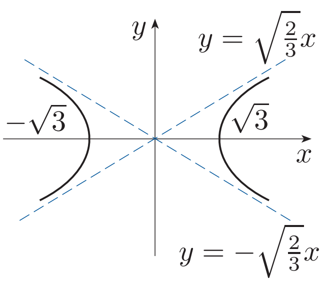
We have $a = \sqrt{3}$ and $b = \sqrt{2}$ so,

$$\begin{aligned} e &= \sqrt{1 - \frac{b^2}{a^2}} \\ &= \sqrt{1 - \frac{2}{3}} \\ &= \sqrt{\frac{1}{3}} = \frac{1}{\sqrt{3}}. \end{aligned}$$

The eccentricity is $1/\sqrt{3}$.

Solution to Exercise A164

We have $a^2 = 3$ and $b^2 = 2$, so $a = \sqrt{3}$ and $b = \sqrt{2}$. The hyperbola with equation $\dfrac{x^2}{3} - \dfrac{y^2}{2} = 1$.



We have $a = \sqrt{3}$ and $b = \sqrt{2}$ so,

$$\begin{aligned} e &= \sqrt{1 + \frac{b^2}{a^2}} \\ &= \sqrt{1 + \frac{2}{3}} \\ &= \sqrt{\frac{5}{3}} = \frac{\sqrt{5}}{\sqrt{3}}. \end{aligned}$$

The eccentricity is $\sqrt{5}/\sqrt{3}$.

Solution to Exercise A165

(a) We can complete the square in the equation

$$x^2 + y^2 - 2x - 6y + 1 = 0$$

to obtain

$$(x-1)^2 - 1 + (y-3)^2 - 9 + 1 = 0,$$

that is,

$$(x-1)^2 + (y-3)^2 = 9.$$

So the equation represents a circle with centre $(1, 3)$ and radius $\sqrt{9} = 3$.

(b) If we complete the square in the equation

$$x^2 + y^2 + x + y + 1 = 0,$$

we obtain the equation

$$\left(x + \tfrac{1}{2}\right)^2 + \left(y + \tfrac{1}{2}\right)^2 = -\tfrac{1}{2}.$$

This equation does not represent a circle: there are no points satisfying it since its left-hand side is always non-negative whereas its right-hand side is negative.

(c) If we complete the square in the equation

$$x^2 + y^2 - 2x + 4y + 5 = 0,$$

we obtain the equation

$$(x-1)^2 + (y+2)^2 = 0.$$

Thus the equation represents the single point $(1, -2)$.

(d) Here the coefficients of x^2 and y^2 are both 2, so we divide the equation by 2 to give

$$x^2 + y^2 + \tfrac{1}{2}x - \tfrac{3}{2}y - \tfrac{5}{2} = 0.$$

If we complete the square in this equation, we obtain the equation

$$\left(x + \tfrac{1}{4}\right)^2 - \tfrac{1}{16} + \left(y - \tfrac{3}{4}\right)^2 - \tfrac{9}{16} - \tfrac{5}{2} = 0,$$

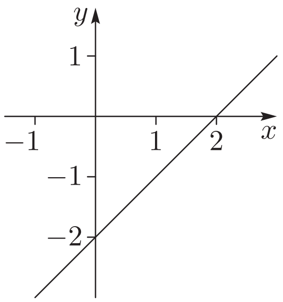
that is,

$$\left(x+\tfrac{1}{4}\right)^2+\left(y-\tfrac{3}{4}\right)^2=\tfrac{25}{8}.$$

Thus the equation represents the circle with centre $\left(-\frac{1}{4},\frac{3}{4}\right)$ and radius $\sqrt{\frac{25}{8}}=\frac{5}{4}\sqrt{2}$.

Solution to Exercise A166

(a) Two points on the line are $(1,-1)$ and $(0,-2)$ (obtained from $t=0$ and $t=-1$, respectively). So the line is as follows.



We eliminate the parameter t by writing $t=x-1$, so $y=(x-1)-1$; that is, the equation of the line is $y=x-2$.

(b) We eliminate the parameter t by writing $t=x/2$ so $y=2(x/2)-2$; that is, $y=x-2$. This shows that the points given by the parametrisation satisfy the equation of the line.

Let (a,b) be any point on the line, so $b=a-2$. Putting $t=a/2$ gives

$$\begin{aligned} g(t)=g(a/2)&=(2(a/2),2(a/2)-2)\\ &=(a,a-2)=(a,b). \end{aligned}$$

Therefore, every point on the line is given by this parametrisation.

Solution to Exercise A167

(a) Setting $(p,q)=(1,2)$ and $(r,s)=(3,6)$ in

$$\alpha(t)=(p+(r-p)t,q+(s-q)t) \text{ for } t\in\mathbb{R}$$

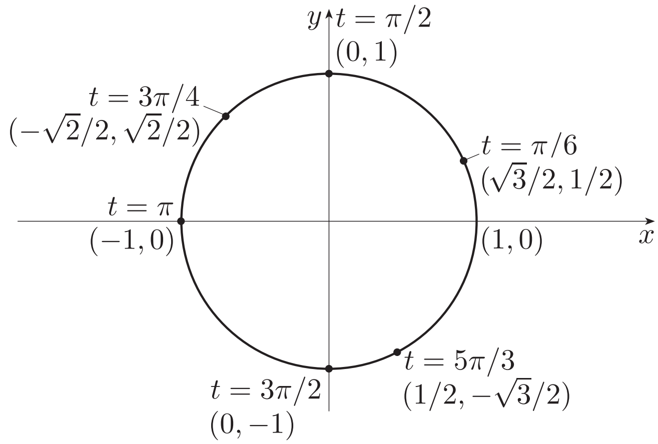
gives

$$\alpha(t)=(1+2t,2+4t),\quad t\in\mathbb{R}.$$

(Other parametrisations are possible.)

(b) $t=\frac{1}{2}$, $t=3$, $t=-\frac{1}{2}$.

Solution to Exercise A168



Solution to Exercise A169

(a) $\alpha(t)=(3\cos t,3\sin t)$, for $t\in[0,2\pi]$.

(b) $\alpha(t)=(2+3\cos t,1+3\sin t)$, for $t\in[0,2\pi]$.

Solution to Exercise A170

(a) $\alpha(t)=\left(\frac{1}{2}t^2,t\right)$, for $t\in\mathbb{R}$.

(b) $\alpha(t)=(\sqrt{3}\cos t,\sqrt{2}\sin t)$, for $t\in[0,2\pi]$.

(c) $\alpha(t)=(\sqrt{3}\sec t,\sqrt{2}\tan t)$, for $t\in[-\pi,\pi]$, excluding $-\pi/2$ and $\pi/2$.

Solution to Exercise A171

The parametric equations for this curve are

$$x = a\cosh t, \quad y = b\sinh t.$$

We eliminate t by writing

$$x/a = \cosh t, \quad y/b = \sinh t$$

and using the identity

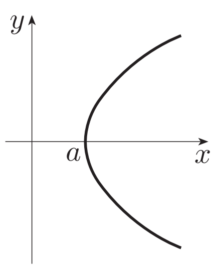
$$\cosh^2 t - \sinh^2 t = 1,$$

to obtain

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1,$$

which is the equation for a hyperbola in standard form.

Since $\cosh t$ is always positive, this parametrisation gives only *one* half of the hyperbola, namely the right-hand half corresponding to positive values of x (because $\cosh t$ takes all values in $[1, \infty)$). Since $\sinh t$ can be positive or negative, we get the *whole* of this right-hand half.



Acknowledgements

Grateful acknowledgement is made to the following sources.

Cover image: © Mark Owen

Unit A1

René Descartes (Subsection 1.1): André Hatala [e.a.] (1997) De eeuw van Rembrandt, Bruxelles: Crédit communal de Belgique. This work is in the public domain in its country of origin and other countries and areas where the copyright term is the author's life plus 100 years or less

André Weil (Subsection 2.2): Taken from: www.xkimdir.com/meslek/matematikci.html

Leonhard Euler (Section 3): Artist: Jakob Emanuel Handmann, image in the public domain

Johann Bernoulli (Section 3): Artist: Johann Rudolf Huber. Image sourced: http://test.maa.org. Found on Wikipedia

Unit A2

Abraham de Moivre (Subsection 2.4): Taken from https://famous-mathematicians.com/abraham-de-moivre/

Carl Friedrich Gauss (Subsection 2.4): Artist: Carl Friedrich Gauß, Öl auf Leinwand (Oil on Canvas), 1840. Image in the public domain

Alexander Ostrowski (Subsection 2.4): Konrad Jacobs, MFO. This file is licensed under the Creative Commons Attribution-Share Alike Licence http://creativecommons.org/licenses/by-sa/3.0/ Germany

Unit A3

Goldbach letter to Euler (Subsection 1.1): Letter from Christian Goldbach to Leonhard Euler 1742. This image is in the public domain

Bourbaki group (Subsection 1.3): © Collection Privee/Archives Charmet/Bridgeman Images

Giuseppe Peano (Subsection 1.5): Photographer unknown. This image is in the public domain

Bertrand Russell (Subsection 1.5): Photographer unknown. This image is in the public domain

Gerhard Gentzen (Subsection 1.5): Eckart Menzler-Trott / https://commons.wikimedia.org/wiki/File:Gerhard_Gentzen.jpg This file is licensed under the Creative Commons Attribution-Noncommercial-ShareAlike Licence http://creativecommons.org/licenses/by-sa/3.0/

Augustus De Morgan (Subsection 2.5): Sophia Elizabeth De Morgan. Image in the public domain

G. H. Hardy (Subsection 3.1): Photographer unknown

Unit A4

Gerardus Mercator (Subsection 4.1): Engraver unknown. This image is in the public domain

Apollonius (Subsection 5.1): Taken from www.maa.org. Image in the public domain

Every effort has been made to contact copyright holders. If any have been inadvertently overlooked the publishers will be pleased to make the necessary arrangements at the first opportunity.

Index